



XpoLog Center V3.0

User Manual

XPOLOG HOME PAGE.....	4
XPOLOG.....	5
LEFT PANE	5
Find	5
Filters	6
Tools	6
Modules	9
Verifiers	11
Enterprise.....	13
MAIN MENU.....	15
Log View.....	15
Problem Diagnostics	20
Portal.....	22
ADMINISTRATION MENU	23
Module.....	23
Log	27
1. Manual configuration:	27
2. Manual XML log configuration:.....	31
3. Windows events log:	34
4. Encrypted text zip archive:.....	35
5. Encrypted XML zip archive:.....	39
6. Merge logs:.....	41
7. Remote XpoLogs:	44
8. Data Base query:	45
9. Add HTTP log configuration:	48
10. Add HTTP XML log configuration:.....	54
11. Add FTP log configuration:	56
12. Add FTP XML log configuration:.....	61
13. Add SSH log configuration:	63
14. Add SSH XML log configuration:	67
15. Automatic configuration wizard:	70
16. Create from Template:.....	76
17. Create from Wizard:	77
Verifier.....	83
CONFIGURATION MENU.....	90
Templates	90
View Templates	90
Saving a template	91
Export Templates	92
Import Templates	92
Wizards.....	93
View Wizards.....	93
Import Wizards	96
Configuration Image	97
Global Customization	106
Global Filters.....	109
DATA SUPPORT MENU.....	111
Export Log.....	111
Import Log.....	116
Export Module	118
Import module.....	121
Import configuration image.....	122
Email text.....	125
Address book.....	126
Enterprise.....	133
Meta Data	135
REPORTS.....	137
Report Definition	137
Report Generation.....	144
SETTINGS MENU.....	146

License	146
Updates	151
UI Settings	151
Log View Settings	152
System Audit	153
Environment Variables	154
Audit	155
About	156
SECURITY	158
User general settings	158
Users view	158
Groups view	160
AUTOMATION MENU	164
Scheduler	164
Define a new Verification Job	164
Define a new Operation Job	167
Tasks	170
Adding a new Execute Task	170
Adding a new Remote Ssh command Task	171
Adding a new URL Task	172
Adding a new Email Task	173
Adding a new Export Module Task	173
Adding a new JMS Message Task	176
Adding a new SNMP Trap Task	178
Adding a new General Report Task	179
XPOSEARCH	181
SEARCH ENGINE	181
Running a Search	181
ADMINISTRATION	184
Log Selection	184
Global Scheduler	184
Delta Scheduler	184
General -	184
INDEXING	185
MANUAL INDEXING	185
DASHBOARD	187
HEALTH VIEW	187
Select Applications	188
Generate Data	189
Time Rule	189
Search	190
Application Status	190
Main Page	190
ADMINISTRATION	192
Defining log risks	192
Defining log statistics	194
Creating Dashboard Data:	195

XpoLog Home page

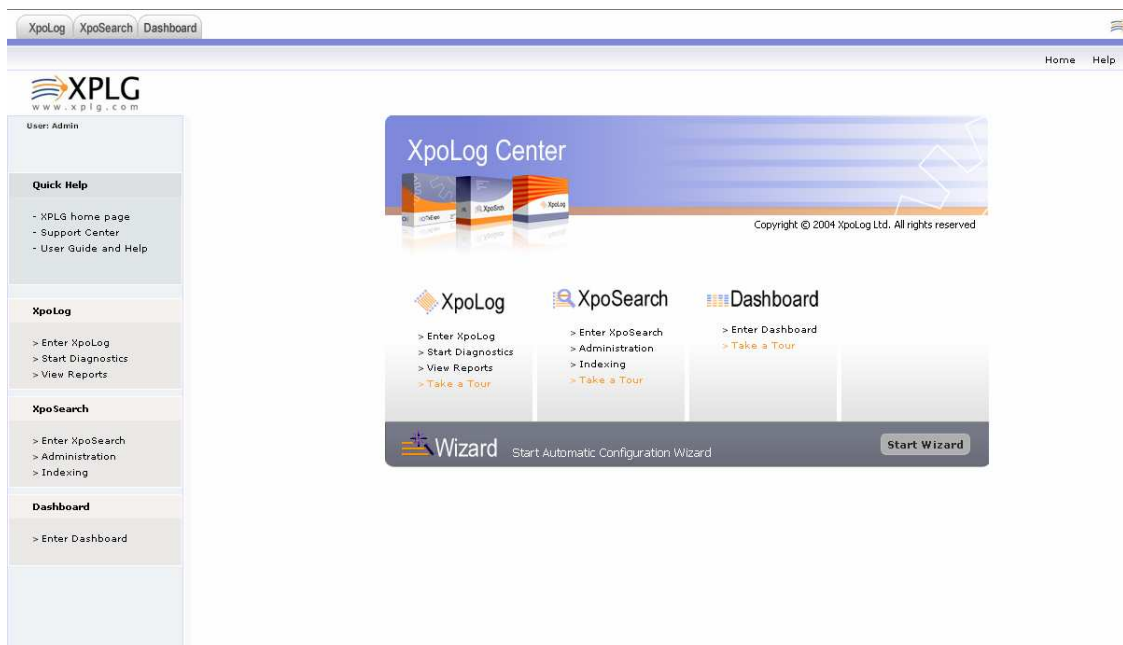
This is the XpoLog's main page. In case security is activated, you will be automatically redirected to a login page.

In the main XpoLog Home page you will find 3 main tabs:

- 1) XpoLog
- 2) XpoSearch
- 3) Dashboard

On the left pane there are a few quick links to XpoLog's help and to the main features as well: XpoLog, XpoSearch and Dashboard.

In the upper right corner there are two links: Home and Help. The Home link will lead back to XpoLog's home page, and Help will open XpoLog's help guide.



XpoLog


Left Pane

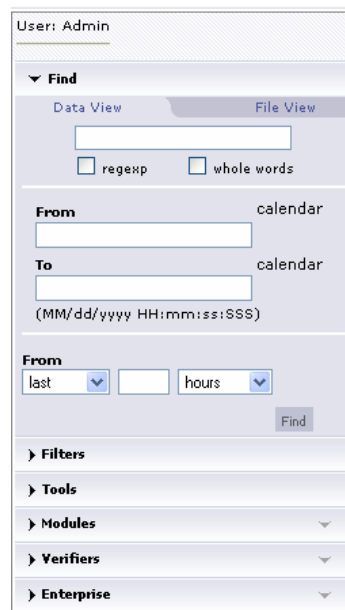
When a log is selected and displayed in the main log view, the left pane is extended to include the following options:

Find

The Find section has two tabs in it: Data view and File view.

The data view acts the same as the quick filter from the log view, with the addition of available time filters that can be set in advance.

The file view displays a list of all the files that are part of the specific log. You can refresh the list by clicking the  icon. You may browse through the list using the up and down arrows.



User: Admin

▼ Find

Data View File View

☐ regex ☐ whole words

From calendar

To calendar

(MM/dd/yyyy HH:mm:ss:SSS)

From

last hours

Find

► Filters

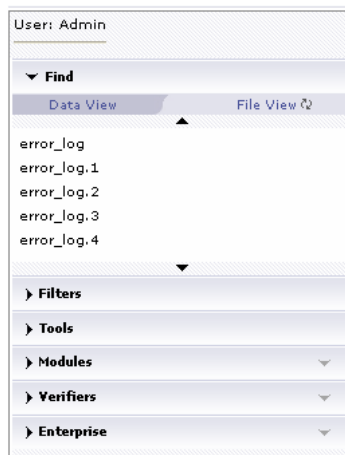
► Tools

► Modules ▼

► Verifiers ▼

► Enterprise ▼

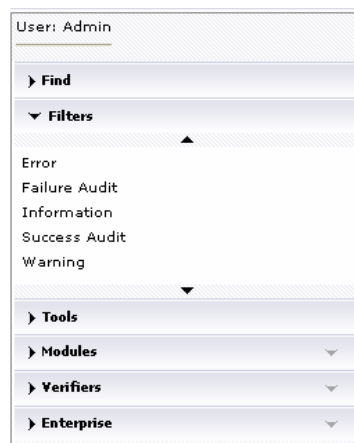
Find – Data View



Find – File view

Filters

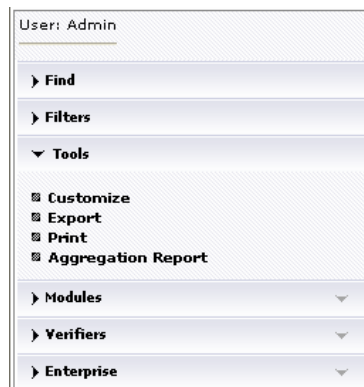
The list of predefined filters is displayed (not quick filters). You may browse through the list using the up and down arrows.



List of available filters

Tools

Inside the tools tab you will find four options: Customize, Export, Print and Aggregation report.



The list of Tools options

- Customize – via this screen you can customize the logs view properties.
 - Table customization: Add/Remove or move Up/Down any column from the available columns list.
 - Priority color selection: If you want events of different priorities to be displayed in different colors, select the ‘Use priority colors’ options; select for each of the priorities in the list a color by clicking on the ‘Pick color’ link and choosing the desired color.
 - Log view settings:
 - Show lines number – check this option in case you would like XpoLog to display line number in the log view.
 - Consolidation – check this option to merge records whose whole data other than the date is identical into one record.
 - Log search settings:
 - Check this option in case you would like XpoLog to present a search and filter result from the beginning of the log
 - Use by default whole words in Search Engine - Checking this option will cause the search engine to search by default for whole words only. Using this option will expedite the searches and filters processes.
 - Log start operation - In case a log is composed of more than one file, you may select the file display order as following:
 - View from the beginning of the most updated file
 - View from the beginning of the oldest file
 - View from the end of the most updated file

- Statistics settings – Check this option in order to allow statistical computations for this log. For more information, go to [Dashboard](#).
- Indexing setting – Check this option to allow faster searches and filtering. For more information, go to [XpoSearch](#) → [Indexing](#).
- Indexing for date search - Check this option to allow fast date searches.
- Search context menu - Add a search context menu to a log by specifying the relevant columns, the name of the data repository (i.e. Google) and the URL to be used for the search.

Log UI Admin

Table customization

Date	Thread	Priority	Logger	Code	Message

[add](#) [remove](#)

Date	Thread	Priority	Logger	Code	Message

[Move up](#) [Move down](#)

Log View Settings

- ☒ Show lines number - when this option is checked you will be able to see the lines number
(Note: unchecking this option will improve performance on browsing to the end of the log)
- ☐ Consolidation - merge similar records.

Log Search Settings

- ☒ When checked - a search and filter result will be presented from the beginning of the log
(Note: when unchecked the result is on current view)
- ☐ Use by default whole words in Search Engine
Checking this option will cause the search engine to search by default for whole words only
this can boost up dramatically search and filter performances

Log Start Operation

When viewing a log that compound of several files,
you may choose from which file to start your view.

- ☒ View from the beginning of the most updated file
- ☐ View from the beginning of the oldest file
- ☐ View from the end of the most updated file

Statistics settings

- ☒ Compute statistics
set this option to enable statistical evaluations on this log

Indexing settings

- ☒ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine
- ☐ Use indexing for date search
set this option to allow for quick date search using the index

Search Context Menu

Column	Name	Path

[Add Menu](#)

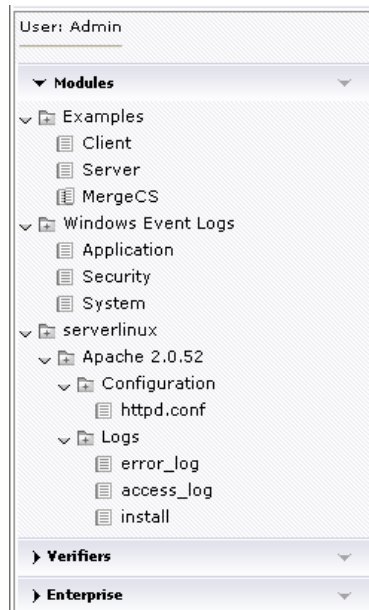
[cancel / back to log viewer](#) [apply](#)

The customize log screen

- Export – Exporting the log using various export methods. For further information, please read about [Data support](#) → [Export log](#).
- Print – Clicking this link will open the log in a separate window ready to print.
- Aggregation Report – This wizard helps you to create a quick aggregation report on the specific log. For further information, please read the Reports chapter.

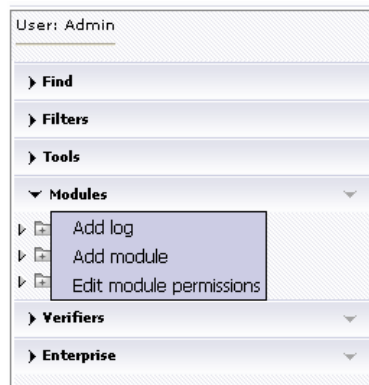
Modules

Under the modules you will find XpoLog's main tree.

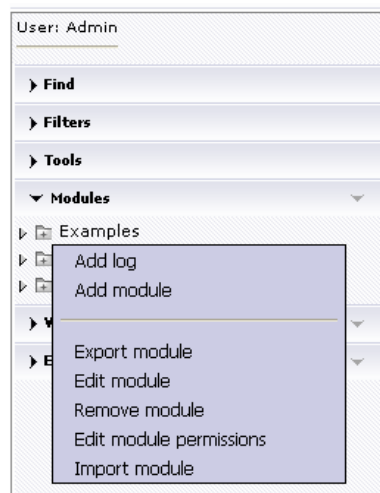


XpoLog tree, located under Modules

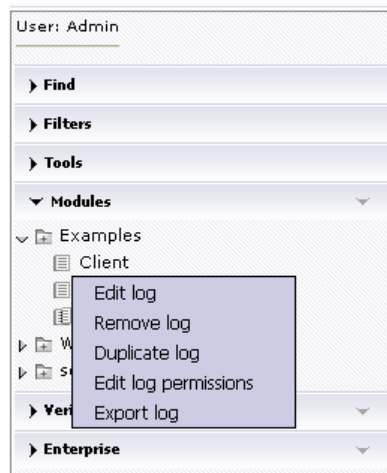
- Click the modules' arrow (▾) in order to add a log, add a module or edit module permissions.
 - Add log – Add a new log to XpoLog. For further information, please go to [Administration → add log](#)
 - Add module – Add a new module to XpoLog. For further information, please go to [Administration → add module](#).
 - Edit module permissions – Edit permission is available only when security is activated. For further information, please go to Security.



- Right click one of the modules. A menu is opened with the following options:
 - Add log – Add a new log to XpoLog. For further information, please go to Administration → add log
 - Add module – Add a new module to XpoLog. For further information, please go to Administration → add module
 - Export module – allows you to export the module with all its data. For further information, please go to Data Support → Export module
 - Edit module – allows you to edit data such as name/owner/parent module and module's members. For further information, please go to Administration → Edit module
 - Remove module – Allows you to remove a module. For further information, please go to Administration → Remove module
 - Import module – Allows you to import a module to XpoLog. For further information, please go to Data support → Import module

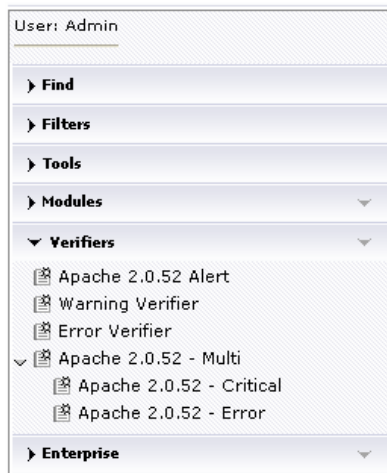


- Right click one of the logs. A menu is opened with the following options:
 - Edit log – Edit an existing log. For further information, please go to Administration → Edit log
 - Remove log – Allows you to remove a log from the system. For further information, please go to Administration → Remove log
 - Duplicate log – Allows you to duplicate the log by going through the log's wizard
 - Export Log – Allows you to export the log using various methods. For further information, please read about Data support → Export log.



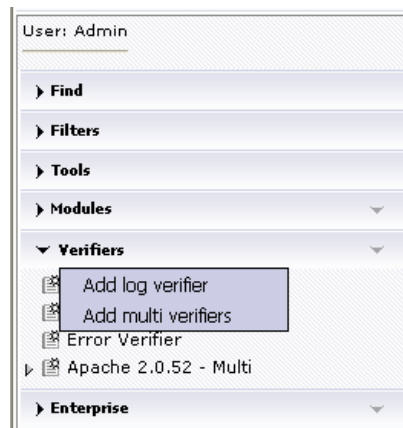
Verifiers

The list of all predefined log verifiers is displayed.

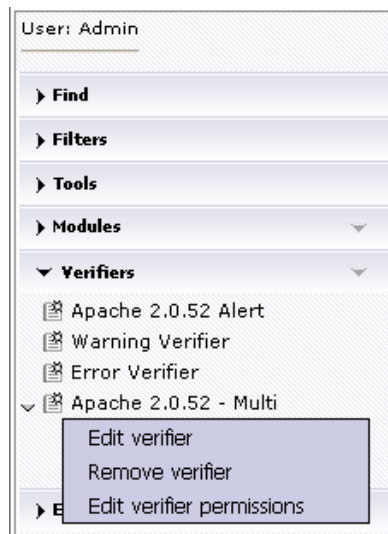


The list of verifiers and multi verifiers in XpoLog

- Click the verifiers' arrow (▼) in order to add a log verifier or add a multi log verifier.
 - Add a log verifier – Add a new log verifier to XpoLog. For further information, please go to Administration → Add verifier
 - Add a multi log verifier – Add a multi log verifier to XpoLog. For further information, please go to Administration → Add verifier

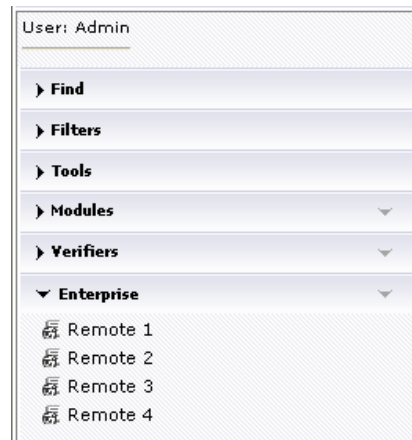


- Right click one of the verifiers. A menu is opened with the following options:
 - Edit verifier – Edit an existing verifier. For further information, please go to Administration → Edit verifier
 - Remove verifier – Allows the user to remove the verifier from the system. For further information, please go to Administration → Remove verifier
 - Edit verifier's permission - Edit permission is available only when security is activated. For further information, please go to Security



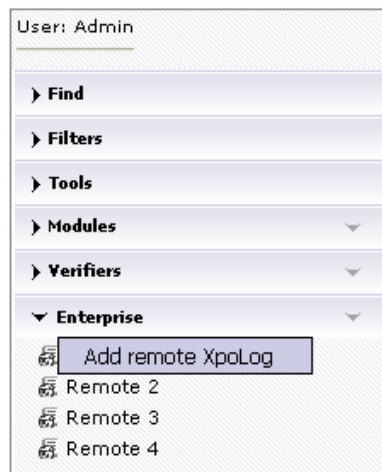
Enterprise

the list of all the remote XpoLogs is displayed.

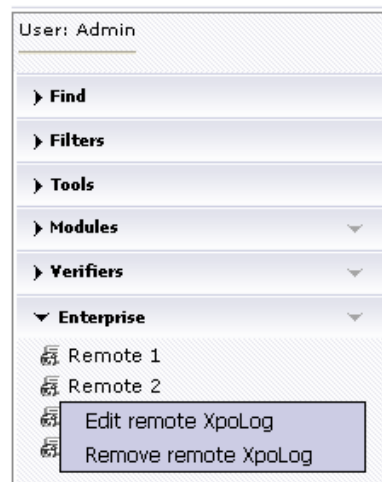


The list of remote XpoLog nodes

- Click the Enterprise's arrow (▼) in order to add a remote XpoLog
 - Add remote XpoLog – allows you to add a remote XpoLog. For further information, please go to Data Support → Enterprise.



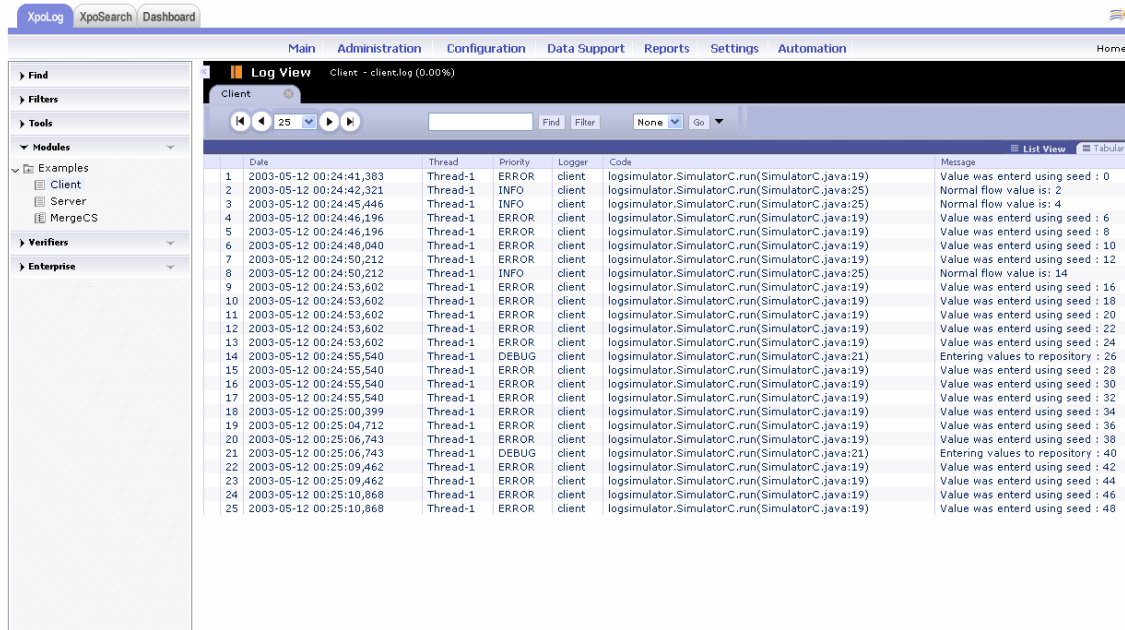
- Right click one of the remote XpoLogs. A menu is opened with the following options:
 - Edit remote XpoLog – Allows you to edit the remote XpoLog details. For further information, please go to Data Support → Enterprise.
 - Remove remote XpoLog - Allows you to remove a remote XpoLog. For further information, please go to Data Support → Enterprise.



Main menu

Log View

Main screen





In order to start viewing a log, click one of the available logs in XpoLog’s tree, located in the left pane under Modules.

Once a log is selected, it is presented in the log view screen.

In the main log view, each log is opened in a separate tab.

In the log’s tab, one will find the following options:

- Navigation . The left arrow will direct the user to the beginning of the log. The next two arrows will display the next records available, according to the ‘number of records to display’ selected in the menu in between those arrows. There are five different display options: 25, 50, 100, 250, and 500 records to display. The last arrow on the right will direct the user to the end of the log.
- Quick find/filter . In order to search a specific string in the log, enter it to the quick find field and click ‘Find’. For example, try searching the phrase: “Error” via the quick filter. The results are highlighted in the log where available:

Main Administration Configuration Data Support Reports Settings Automation Home Help						
Log View Client - client.log (0.00%)						
Client						
<div> <div> <div>25</div> <div> <div></div> <div></div> <div></div> </div> </div> <div> <div>error</div> <div>Find</div> <div>Filter</div> <div>None</div> <div>Go</div> </div> </div>						
List View Tabular View						
	Date	Thread	Priority	Logger	Code	Message
1	2003-05-12 00:24:41,383	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 0
2	2003-05-12 00:24:42,321	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 2
3	2003-05-12 00:24:45,446	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 4
4	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 6
5	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 8
6	2003-05-12 00:24:48,040	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 10
7	2003-05-12 00:24:50,212	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 12
8	2003-05-12 00:24:50,212	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 14
9	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 16
10	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 18
11	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 20
12	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 22
13	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 24
14	2003-05-12 00:24:55,540	Thread-1	DEBUG	client	logsimulator.SimulatorC.run(SimulatorC.java:21)	Entering values to repository : 26
15	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 28
16	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 30
17	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 32
18	2003-05-12 00:25:00,399	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 34
19	2003-05-12 00:25:04,712	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 36
20	2003-05-12 00:25:06,743	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 38
21	2003-05-12 00:25:06,743	Thread-1	DEBUG	client	logsimulator.SimulatorC.run(SimulatorC.java:21)	Entering values to repository : 40
22	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 42
23	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 44
24	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 46
25	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 48

In case you want to see only the relevant searched results, the filter command should be used. Enter the same phrase to the quick filter field, and click filter. The results should be displayed in the following way:

Main Administration Configuration Data Support Reports Settings Automation Home Help						
Log View Client - client.log (0.12%)						
Client						
<div> <div> <div>25</div> <div> <div></div> <div></div> <div></div> </div> </div> <div> <div></div> <div>Find</div> <div>Filter</div> <div>Error</div> <div>Go</div> </div> </div>						
List View Tabular View						
	Date	Thread	Priority	Logger	Code	Message
4	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 6
5	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 8
6	2003-05-12 00:24:48,040	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 10
7	2003-05-12 00:24:50,212	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 12
9	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 16
10	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 18
11	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 20
12	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 22
13	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 24
15	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 28
16	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 30
17	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 32
18	2003-05-12 00:25:00,399	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 34
19	2003-05-12 00:25:04,712	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 36
20	2003-05-12 00:25:06,743	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 38
22	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 42
23	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 44
24	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 46
25	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 48
27	2003-05-12 00:25:15,477	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 52
28	2003-05-12 00:25:15,477	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 54
29	2003-05-12 00:25:15,477	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 56
30	2003-05-12 00:25:16,321	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 58
31	2003-05-12 00:25:18,930	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 60
32	2003-05-12 00:25:18,930	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 62

- Predefined filters. Click the small arrow in order to open the filter's menu. Click 'New' the following screen is displayed:

Filter definition

Name

GenFilterName_1

☒ use search engine

Description

Priorities

From name

DEBUG

INFO

WARN

ERROR

FATAL

add

add all

remove

remove all

To name

Date and Time

☒ Dates limit

☐ Show records that arrive after

07/22/2007 11:18:04

calendar

(MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH:mm:ss:SSS)

☐ Show records that arrive before

07/22/2007 11:18:04

calendar

(MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH:mm:ss:SSS)

☐ show records from the

last

hours

Text

Show records that

contain

the text

☐

☐

☐

Show records that

contain

the text

☐

☐

☐

Show records that

contain

the text

☐

☐

☐

Show records that

contain

the text

☐

☐

☐

☒ search in all columns

☐ search in these columns

Columns

Date

Thread

Priority

Logger

Code

Message

add

add all

remove

remove all

Only

System Health

Risk Weight:

None

if there are

More Than

0

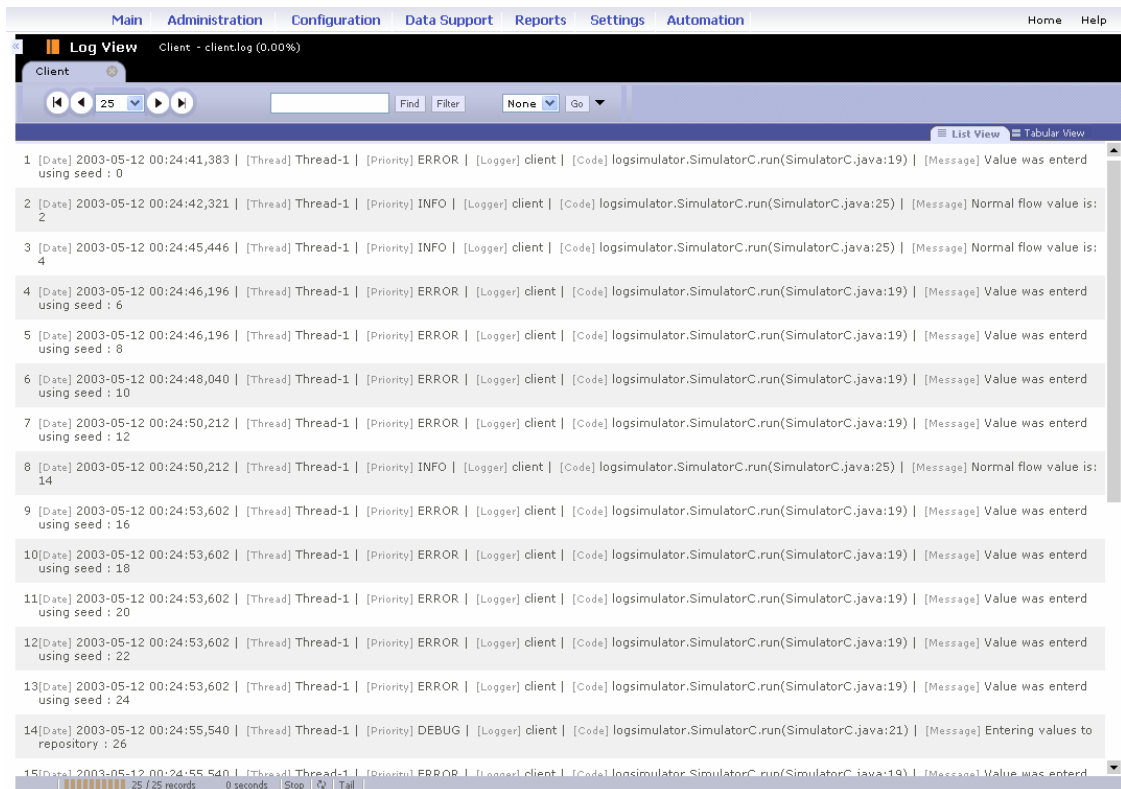
records in a time frame of 5 minutes.


save

cancel



help

- In the first section, you should provide a name to the filter and a description (Not mandatory).
- In the second part of the wizard, you can select a predefined priority according to the log's pattern.
- You may narrow down the filter to a specific time frame using the date and time rules.
- In the fourth part (Text), you may add any desired string to be filtered. You may add a filter that Contains/Not Contains/Equals/Not Equals a relevant string. Moreover, you can decide if the filtered string should be searched in all columns or from specific column/columns, by adding the relevant column to the 'only' list. When the filter definition is complete, click save. XpoLog will lead you back to the main log view screen, displaying only the filtered results.
- List View/Tabular view. You may switch between both views for your own comfort. The default view is the Tabular view. The list view will look like this:



- At the bottom of the log viewer screen you will find a progress bar, the number of records found, the time it took XpoLog to find and display the records, Stop, Refresh and Tail links. 

The tail command is used to update the log's data in real time. It will look for new records to display every X seconds and will display them as soon as they reach a certain minimum number of records. For more info, please see: Log view settings.

- In order to open the log view in a full screen mode, click the arrows link, located in the upper left side of the log view - . In order to return to the normal view, click the  link again:

	Date	Thread	Priority	Logger	Code	Message
1	2003-05-12 00:24:41,383	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 0
2	2003-05-12 00:24:42,321	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 2
3	2003-05-12 00:24:45,446	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 4
4	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 6
5	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 8
6	2003-05-12 00:24:48,040	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 10
7	2003-05-12 00:24:50,212	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 12
8	2003-05-12 00:24:50,212	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 14
9	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 16
10	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 18
11	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 20
12	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 22
13	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 24
14	2003-05-12 00:24:55,540	Thread-1	DEBUG	client	logsimulator.SimulatorC.run(SimulatorC.java:21)	Entering values to repository : 26
15	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 28
16	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 30
17	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 32
18	2003-05-12 00:25:00,399	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 34
19	2003-05-12 00:25:04,712	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 36
20	2003-05-12 00:25:06,743	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 38
21	2003-05-12 00:25:06,743	Thread-1	DEBUG	client	logsimulator.SimulatorC.run(SimulatorC.java:21)	Entering values to repository : 40
22	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 42
23	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 44
24	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 46
25	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 48

- Right clicking the main log view will open a menu with the following options:
 - Find/Filter – Same as the quick find/filter described above.
 - Search → XpoSearch/Google.

The specific string that was right clicked (from the log) can be searched in one of the following methods:

- 1) XpoSearch: For further details, read the XpoSearch chapter
- 2) Google: A new window is opened with the relevant string search results in Google.

	Date	Thread	Priority	Logger	Code	Message
1	2003-05-12 00:24:41,383	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 0
2	2003-05-12 00:24:42,321	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 2
3	2003-05-12 00:24:45,446	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 4
4	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 6
5	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 8
6	2003-05-12 00:24:48,040	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 10
7	2003-05-12 00:24:50,212	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 12
8	2003-05-12 00:24:50,212	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 14
9	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 16
10	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 18
11	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 20
12	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 22
13	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 24
14	2003-05-12 00:24:55,540	Thread-1	DEBUG	client	logsimulator.SimulatorC.run(SimulatorC.java:21)	Entering values to repository : 26
15	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 28
16	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 30
17	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 32
18	2003-05-12 00:25:00,399	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 34
19	2003-05-12 00:25:04,712	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 36
20	2003-05-12 00:25:06,743	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 38
21	2003-05-12 00:25:06,743	Thread-1	DEBUG	client	logsimulator.SimulatorC.run(SimulatorC.java:21)	Entering values to repository : 40
22	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 42
23	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 44
24	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 46
25	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was entered using seed : 48

- Customize/Export/Print/Aggregation Report. For more details, please read about tools in the left pane.

Problem Diagnostics

User: Admin

Navigation: Main, Administration, Configuration, Data Support, Reports, Settings, Security, Automation, Home, Help

Problem Isolation Process

Problem Time Frame (+/-)

☒ All Data

☐ Dates limit (MM/dd/yyyy HH:mm:ss)

Start: 07/23/2007 10:53:38 [calendar](#)

End: 07/23/2007 10:53:38 [calendar](#)

☐ Data: from the last [] minutes

Problem Related Search Terms (+/-)

Enter a search term. Use ',' to separate between terms

Problem Related Applications & Logs (+/-)

Select the applications and logs that the problem occurred in

☐ other

☒ Examples

☐ Client

☐ Server

☐ MergeCS

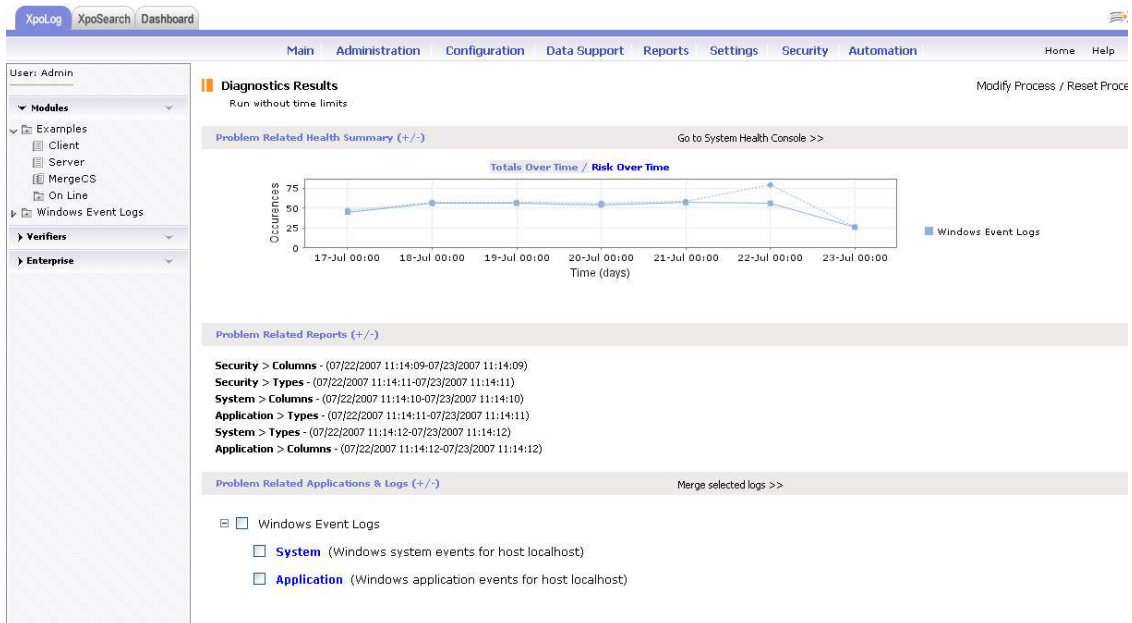
☐ On Line

[Go >](#)

The problem diagnostics is where the problem isolation process starts.

Configure the relevant time frame, terms, and select the relevant logs.

When done, click ‘Go’.



The result of this process provides the following data:

- **Health summary:** The health summary graph provides both the total events occurred during a specific time frame and the risk level, during that time. For more comprehensive analysis, in the Dashboard, click the ‘Go to system health console’. For further information, please refer to the Dashboard chapter.

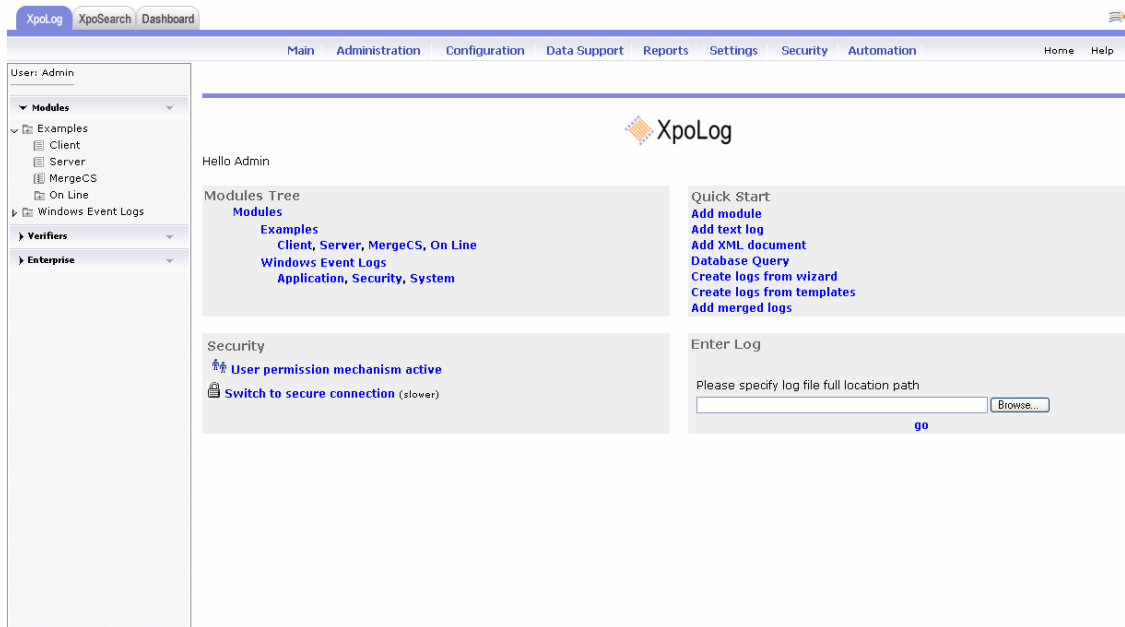
- Related reports: A list of relevant available reports in XpoLog is presented. Each report can be accessed by clicking its name. For further information, please refer to the Reports chapter.
- Related Applications and logs: A list of relevant available logs in XpoLog is presented. Each log can be accessed by clicking its name. In case there is more than one log related, XpoLog can merge them into one log and present them in the log viewer. In order to do so, select the desired logs, and click 'Merge selected logs'.

In the upper right corner of the screen you will find two links: Modify process and Reset process.

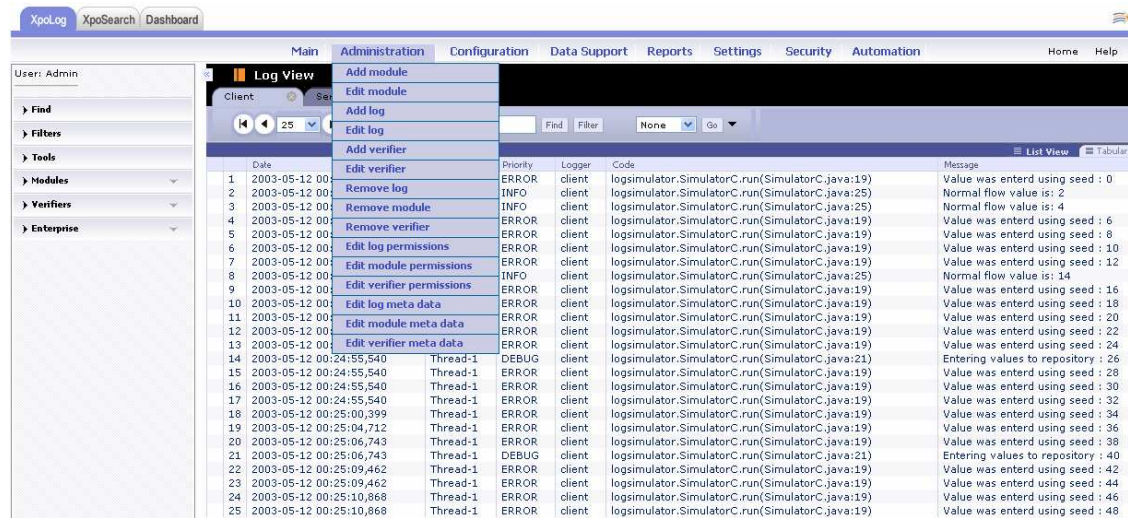
Use the first one in order to reconfigure the problem isolation process, or use the 'Reset process' in case you would like to start a new problem isolation process.

Portal

This is XpoLog's portal. It is about to change soon.



Administration Menu



The administration menu can be divided into 3 main substances:

- 1) Module – Add/Edit/Remove/Permission¹/Meta data
- 2) Log - Add/Edit/Remove/Permission/Meta data
- 3) Verifier - Add/Edit/Remove/Permission/Meta data

Module

- **Add module** – In order to add a new module, open the administration menu, and click ‘Add module’. Select a parent module and add a module’s name. You can add an owner and description for the module if desired. When finished, click ‘Save’.

¹ Permission is presented only when Security is activated.

A message indicating that the operation ended successfully will be presented. Click ‘Ok’.

- **Edit module** – In order to edit an existing module via the administration menu, the specific module should be in focus. Select the relevant module in the left pane in the log viewer. When the module is in focus, open the administration menu and click ‘Edit module’. Edit the module’s properties and click save when done.
- **Edit module’s permissions** – Editing the module’s permissions enables you to set edit/view permissions for specific users/groups. . Editing the module’s permissions is only available when security is activated. For further information

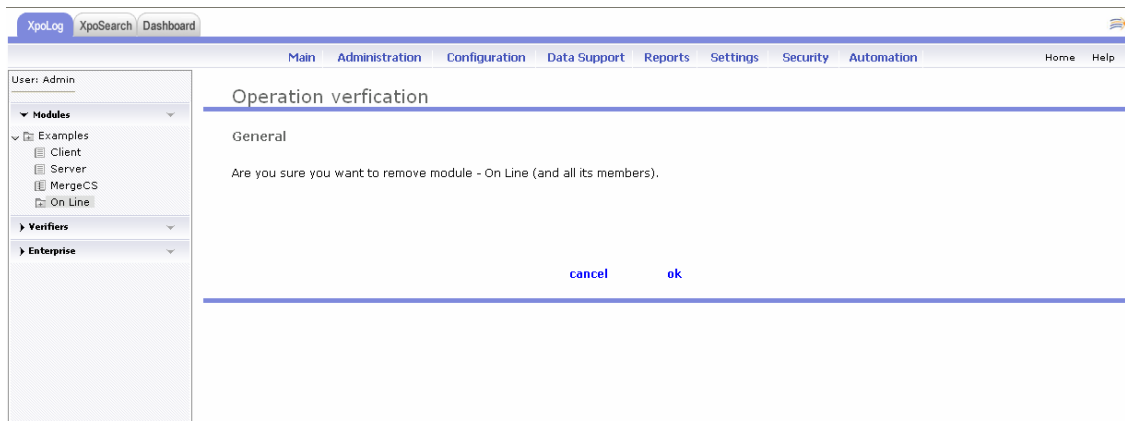
on security, please refer to Settings → General. Open the administration menu, and click ‘Edit module permission’.

There are two options to set permissions:

1. ‘Parent permissions’ – this will set the same permissions as set in the parent module.
2. ‘Use specified permissions’ – selecting this option will allow you to add or remove users/groups from both available options: Edit group and the View group.

Click ‘Reset’ in case you would like to discard all changes, or click ‘Apply’ in order to save changes.

- **Edit module’s Meta data** – this option will be available only if module’s Meta data was added in advance. For further information, please go to Data support → Meta data.
- **Remove module** – in order to remove a module, open the administration menu, and click ‘Remove module’. Clicking ‘Ok’ will confirm deletion of module. In case you don’t want to delete it, click ‘Cancel’.



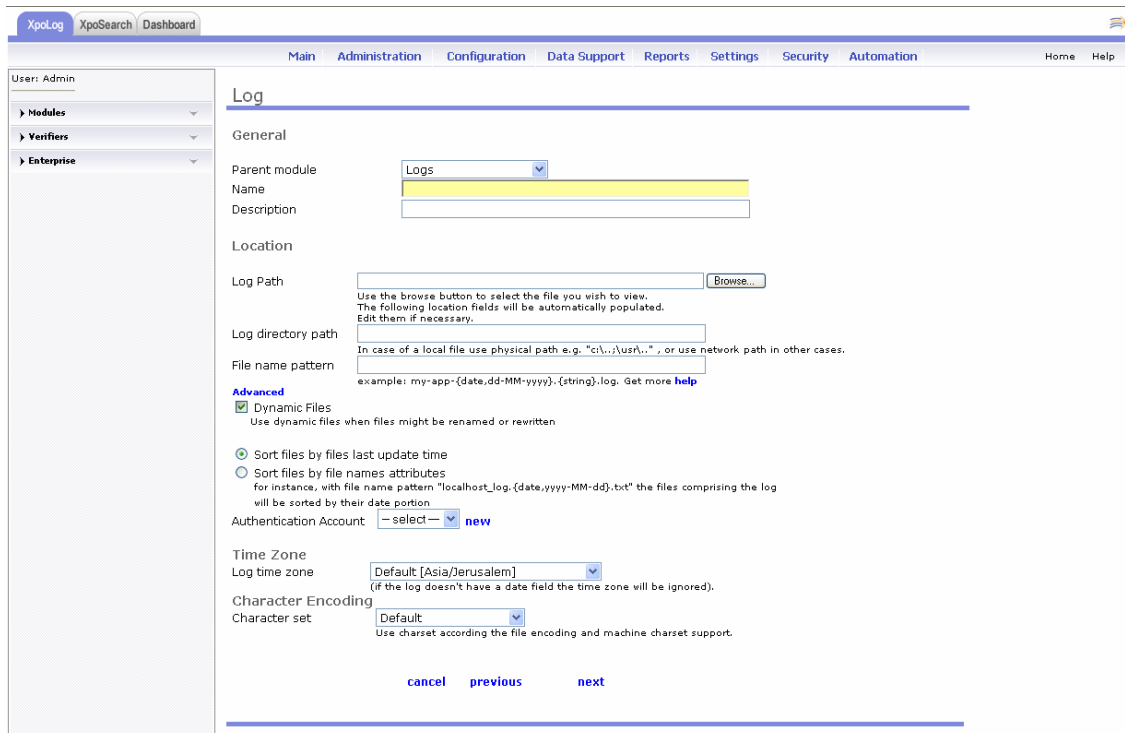
Log

- **Add log** – In order to add a new log to XpoLog, open the administration menu and select ‘Add log’. There are quite a few different logs that can be added to the XpoLog, in different methods.



The list of logs that can be added to the XpoLog

1. Manual configuration:



The first screen of the add log wizard

In order to manually add a regular log, select the manual configuration option. Select the parent module for this log, and configure the following General data: Name, Description.

Enter the log's path and the log directory path and file name pattern will be populated automatically. You can also configure the log directory path and the log's pattern directly.

Advanced - Dynamic files – Select this option in case the files might be renamed or overwritten.

Sort files – Select the first option in order to sort files by date.

In case you would like to sort the files by names attributes, select the second option.

Authentication Account – select the appropriate account if one is needed to access files located on a remote machine.

Moreover, it is possible to set the logs time zone as well as its character encoding. At this point you have two options: Click save, and skip the rest of the log wizard, or click next in order to continue configuring the log.

The next wizard screen is the log pattern administration:

Log pattern administration

Text from the log file

Few lines from the log file you specified.

```
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:45:05,375] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:45:05,390] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:57:18,187] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task SearchEngineIntervalIndex
[2007-07-22 10:00:00,031] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task XpoLogRemoteSessionMain
```

Log line/record pattern

Here you need to specify the pattern description of the log records. Be as accurate as you can for best analysis.

{string}

examples: {date,dd-MM-yyyy}-{number}-{(string)} (priority,DEBUG:INFO;WARN:ERROR) - {string} [pattern help](#)
 you can insert more than one pattern on the log, just separate between patterns by starting each pattern in a new line [multi-pattern help](#)

[verify pattern](#) [get pattern suggestions](#)

Advanced

Header settings

Look for header in the first lines

you can insert here a pattern of header which describe the log. [header settings help](#)

Log View settings

☐ Ignore unparsed records - when this option is checked you will see only records that fit the above pattern

☐ Show lines number - when this option is checked you will be able to see the lines number
 (Unchecked this will improve performance when going to the end of a log)

Pattern verification status

Analysis result of the log lines with the data pattern

Syntax verification - **ok**

Log analysis verification - **ok**

Log records analysis result

Here you can see the log lines after they were analyzed using the data pattern.

Text 1
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:45:05,375] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:45:05,390] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:57:18,187] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task SearchEngineIntervalIndex
[2007-07-22 10:00:00,031] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task XpoLogRemoteSessionMaintenance
[2007-07-22 10:03:58,468] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client
[2007-07-22 10:05:50,875] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client

The second screen of the add log wizard

A few lines from the log are presented in the ‘Text from the log file’ window. In the ‘Log line/Record pattern’ you need to add a pattern for the selected log. When done adding the desired pattern, click ‘Verify pattern’ to make sure that it was added correctly. The ‘pattern verification status’ will indicate whether the pattern is legal or not.

Pattern verification status
 Analysis result of the log lines with the data pattern
 Syntax verification - **ok**
 Log analysis verification - **ok**

The ‘Log records analysis result’ will display a few lines from the parsed log.

Header settings – set the number of lines according the log’s header length in case you wish XpoLog to disregard the log’s header.

You may add a separate pattern for the header as well.

Log view settings – Check the ‘Ignore unparsed records’ if you do not want XpoLog to show you records that does not match the log’s pattern. Check

the ‘Show line number’ in case you want to see the log’s line numbers
(NOTE: This option will slow down XpoLog a bit).

Click next in order to move on to the last screen of the log’s wizard:

User: Admin

Navigation: XpoLog | XpoSearch | Dashboard

Main | Administration | Configuration | Data Support | Reports | Settings | Security | Automation | Home | Help

Log field admin

Generated table

Date	Text 2	Priority	Text 4	Text 5	Text 6
2007-07-22 09:42:31,156	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologReports
2007-07-22 09:42:31,156	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologMaintenance
2007-07-22 09:45:05,375	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologReports

Field specification

Field Type	Field Name
1. date	Date
2. string	Text 2
3. priority	Priority
4. string	Text 4
5. string	Text 5
6. string	Text 6

Virtual columns [Add virtual column](#)

Statistics settings
☐ Compute statistics
 set this option to enable statistical evaluations on this log

Indexing settings
☐ Use indexing
 using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine

[cancel](#) [previous](#) [next](#)

The third screen of the add log wizard

In this screen you can set the columns name, add a virtual column and set the statistics/indexing settings.

Rename columns – in the field name, enter the desired column name.

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.

Add Virtual Column

Operation: Merge

Columns: Text 2, Priority, Text 4, Text 5, Text 6

[cancel](#) [add](#)

The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.

Field specification

	Field Type	Field Name		Compute statistics:
1.	date	Date		do not compute
2.	string	Text 2		do not compute
3.	priority	Priority		do not compute
4.	string	Text 4		do not compute
5.	string	Text 5		do not compute
6.	string	Text 6		do not compute

Virtual columns [Add virtual column](#)

Statistics settings

☒ Compute statistics
set this option to enable statistical evaluations on this log

Statistical computation settings can be applied to each column separately

Indexing setting: check the 'Use indexing' in order to index the log. When the 'use indexing' is marked, a second indexing option appears: 'Use indexing for date search'. For further information, please refer to XpoSearch.

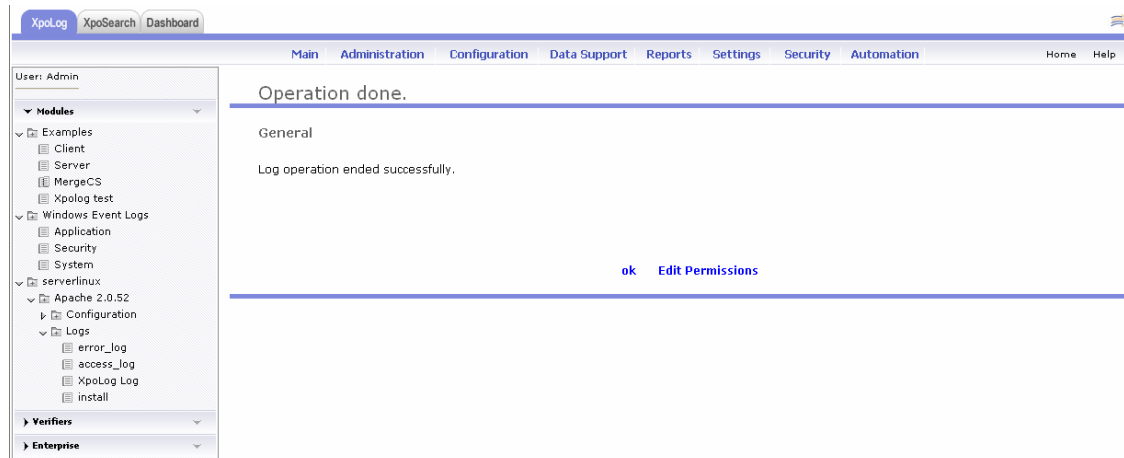
Indexing settings

☒ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine

☐ Use indexing for date search
set this option to allow for quick date search using the index

When done configuring the indexing, click 'Next'.

The log's wizard is done; Click OK to end the wizard. In case security is activated, you may edit the log's permissions by clicking 'Edit Permissions'.



2. Manual XML log configuration:

The screenshot shows the XpoLog configuration interface. The top navigation bar includes tabs for XpoLog, XpoSearch, and Dashboard, and a menu with options like Main, Administration, Configuration, Data Support, Reports, Settings, Security, and Automation. The sidebar on the left shows a tree view of modules and verifiers. The main configuration area is titled 'Log' and contains the following fields:

- General**
 - Parent module: Examples (dropdown)
 - Name: (text input)
 - Description: (text input)
- Location**
 - Log Path: (text input) [Browse...](#)
 - Log directory path: (text input)
 - File name pattern: (text input)
- Time Zone**
 - Log time zone: Default [Asia/Jerusalem] (dropdown)
- Record Tag Name**
 - Tag name: (text input)
- Character Encoding**
 - Character set: Default (dropdown)

At the bottom of the configuration area, there are three buttons: [cancel](#), [previous](#), and [next](#).

In order to add an XML log, select the manual XML log configuration option. Select the parent module for this log, and configure the following General data: Name, Description.

Enter the log's path and the log directory path and file name pattern will be populated automatically. You can also configure the log directory path and the log's pattern directly.

Set the logs time zone, the record tag name and the character encoding.

Click next in order to continue configuring the log.

In the second wizard's screen you will need to configure the XML log schema by specifying for each field type and name a pattern and a condition according to the XML code above. If there are missing elements or attributes please add them to the structure above and click the 'Reanalyze XML code'.

XpoLogXpoSearchDashboard

User: Admin

Modules

Examples

Client

Server

MergeCS

Xpolog test

Windows Event Logs

Application

Security

System

serverlinux

Apache 2.0.52

Configuration

Logs

error_log

access_log

XpoLog Log

install

Verifies

Enterprise

MainAdministrationConfigurationData SupportReportsSettingsSecurityAutomation

HomeHelp

XML Log schema administration

Text from the XML file

The first log element from the XML log file you specified.

```
<event logger="com.brio.one.mgmt.logging.LoggingManager" timestamp="1062802538234" level="ALWAYS" thread="Fo
<time>05 Sep 2003 15:55:38,234</time>
<context originator_type="CommonServices" originator_name="BrioPlatform_sla1_sla1_1800" host="sla1" />
<message>*****
</message>
</event>
```

reanalyze XML code

XML schema definition

Here you need to specify for each field type and name according to the XML code above

If there are missing elements or attributes please add them to the structure above and click on [reanalyze XML code](#)

Tag Name	Attribute	Value - XpoLog pattern	condition	Ignore	Tags Included
1. event		{string}	No Selected =	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2. event	logger	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
3. event	timestamp	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
4. event	level	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
5. event	thread	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
6. event	sequence_no	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
7. time		{string}		<input type="checkbox"/>	<input type="checkbox"/>
8. context		{string}	No Selected =	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9. context	originator_type	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
10. context	originator_name	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
11. context	host	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
12. message		{string}		<input type="checkbox"/>	<input type="checkbox"/>

pattern examples: {date,dd-MM-yyyy}, {number}, {string}, {priority,DEBUG;INFO;WARN;ERROR}

pattern help

Use the ‘Verify Schema’ to see a preview of the analyzed log according to the given pattern.

verify schema

Pattern verification status

Analysis result of the log lines with the data pattern

Log analysis verification - **ok**

Log records analysis result

Here you can see the log view after the xml log was analyzed the schema

	logger	timestamp	level	thread	sequence_no	time	originator_type	originator_
	com.brio.one.mgmt.logging.LoggingManager	1062802538234	ALWAYS	Foundation Server	0	05 Sep 2003 15:55:38,234	CommonServices	BrioPlatf
	com.brio.one.mgmt.logging.LoggingManager	1062802538265	ALWAYS	Foundation Server	1	05 Sep 2003 15:55:38,265	CommonServices	BrioPlatf
	com.brio.one.mgmt.logging.LoggingManager	1062802538281	ALWAYS	Foundation Server	2	05 Sep 2003 15:55:38,281	CommonServices	BrioPlatf

cancel

previous

next

Click ‘next’ to move on to the last wizard’s screen, where you will have to configure the field specification, virtual columns and statistics computation.

33

XpoLog XpoSearch Dashboard

Main Administration Configuration Data Support Reports Settings Automation Home

Modules

- Examples
 - Client
 - Server
 - MergeCS
 - Merge
 - Win Event Application
 - Win event merge
 - HTTP
- Windows Event Logs
 - serverlinux
 - serverwin
 - qaserver
 - serverdb
- Test
 - XpoLog log
 - XpoAudit
 - XpoMerge
 - Win Event Merge
 - win event
 - Merge from XpoSearch
 - 663
 - Bug 663
 - qa1
 - ziv
 - amirn
 - remote serverlinux
 - test
 - DB Query
- Verifiers
- Enterprise

Log field admin

Generated table

	logger	timestamp	level	thread	sequence_no	time	originator_type	originator_name
	com.brio.one.mgmt.logging.LoggingManager	1062802538234	ALWAYS	Foundation Server	0	05 Sep 2003 15:55:38,234	CommonServices	BrioPlatform,
	com.brio.one.mgmt.logging.LoggingManager	1062802538265	ALWAYS	Foundation Server	1	05 Sep 2003 15:55:38,265	CommonServices	BrioPlatform,
	com.brio.one.mgmt.logging.LoggingManager	1062802538281	ALWAYS	Foundation Server	2	05 Sep 2003 15:55:38,281	CommonServices	BrioPlatform,

Filed specification

Field Type	Field Name	
1. string	logger	<input type="checkbox"/> Compute statistics on this column
2. string	timestamp	<input type="checkbox"/> Compute statistics on this column
3. string	level	<input type="checkbox"/> Compute statistics on this column
4. string	thread	<input type="checkbox"/> Compute statistics on this column
5. string	sequence_no	<input type="checkbox"/> Compute statistics on this column
6. string	time	<input type="checkbox"/> Compute statistics on this column
7. string	originator_type	<input type="checkbox"/> Compute statistics on this column
8. string	originator_name	<input type="checkbox"/> Compute statistics on this column
9. string	host	<input type="checkbox"/> Compute statistics on this column
10. string	message	<input type="checkbox"/> Compute statistics on this column

Virtual columns [Add virtual column](#)

Statistics settings

☒ Compute statistics
set this option to enable statistical evaluations on this log

[cancel](#) [previous](#) [next](#)

Click 'next' in order to finish the log's wizard. You may also go back, using the 'previous' link, and reconfigure the log's properties.

3. Windows events log:

XpoLog XpoSearch Dashboard

Main Administration Configuration Data Support Reports Settings Automation Home

Modules

- Examples
- Windows Event Logs
 - serverlinux
 - serverwin
 - qaserver
 - serverdb
- Test
- Verifiers
- Enterprise

Log

General

Parent module:

Name:

Description:

Location

Machine name:
Please put empty machine name for using localhost

Log Name:

☒ Application ☐ System ☐ Security

☐ Custom:
Notice: If a custom registered log name cannot be found, the event logging service will open the Application log

☐ File: from type:

Time Zone

Log time zone:
(if the log doesn't have a date field the time zone will be ignored).

Character Encoding

Character set:
Use charset according the file encoding and machine charset support.

[cancel](#) [previous](#) [Finish](#)

In order to add a Windows event log, select the 'Windows event log' configuration option. Select the parent module for this log, and configure the following General data: Name and Description.

Enter the machine name, or leave it empty in case the logs are located in localhost. Specify the log type: Application, System or Security.

A different option would be select 'File' and add the relevant path manually along with the log's type.

Set the logs time zone and the character encoding.

When done configuring the Windows event log, click 'Finish' to exit the wizard.

4. Encrypted text zip archive:

The screenshot shows the 'Log' configuration wizard in the XpoLog application. The interface includes a sidebar with a tree view of modules (Examples, Windows Event Logs, serverlinux, serverwin, qaserver, serverdb, Test) and verifiers (Enterprise). The main area is titled 'Log' and contains several sections: 'General' with fields for Parent module (Examples), Name, and Description; 'Location' with fields for Log Path (with a 'Browse...' button), Log directory path, and File name pattern (with an example: my-app-{date,dd-MM-yyyy}.(string).log); 'Advanced' with fields for Time Zone (Default [Asia/Jerusalem]), Log time zone, Character Encoding (Default), and Character set; and 'Encrypted Zip Password' with a Password field. At the bottom, there are 'cancel', 'previous', and 'next' buttons.

In order to manually add an encrypted zip log, select the 'Encrypted text zip archive' option. Select the parent module for this log, and configure the following General data: Name, Description.

Enter the log's path and the log directory path and file name pattern will be populated automatically. You can also configure the log directory path and the log's pattern directly.

Advanced - Dynamic files – Select this option in case the files might be renamed or overwritten.

Sort files – Select the first option in order to sort files by date.

In case you would like to sort the files by names attributes, select the second option.

Authentication Account – select the appropriate account if one is needed to access files located on a remote machine.

Moreover, it is possible to set the logs time zone as well as its character encoding. Finally, add the encrypted zip password.

Click next in order to continue to the next wizard's screen.

User: Admin

Modules Verifiers Enterprise

Main Administration Configuration Data Support Reports Settings Security Automation Home Help

Log pattern administration

Text from the log file

Few lines from the log file you specified.

```
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:45:05,375] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:45:05,390] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:57:18,187] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task SearchEngineIntervalIndex
[2007-07-22 10:00:00,031] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task XpoLogRemoteSessionMain
```

Log line/record pattern

Here you need to specify the pattern description of the log records. Be as accurate as you can for best analysis.

{string}

examples: {date,dd-MM-yyyy}-{number}-{string} {priority,DEBUG;INFO;WARN;ERROR} - {string} [pattern help](#)
you can insert more than one pattern on the log, just separate between patterns by starting each pattern in a new line [multi-pattern help](#)

[verify pattern](#) [get pattern suggestions](#)

Advanced

Header settings

Look for header in the first lines

you can insert here a pattern of header which describe the log. [header settings help](#)

Log View settings

☐ Ignore unparsed records - when this option is checked you will see only records that fit the above pattern

☐ Show lines number - when this option is checked you will be able to see the lines number
(Unchecked this will improve performance when going to the end of a log)

Pattern verification status

Analysis result of the log lines with the data pattern

Syntax verification - **ok**

Log analysis verification - **ok**

Log records analysis result

Here you can see the log lines after they were analyzed using the data pattern

Text 1
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:45:05,375] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:45:05,390] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:57:18,187] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task SearchEngineIntervalIndex
[2007-07-22 10:00:00,031] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task XpoLogRemoteSessionMaintenance
[2007-07-22 10:03:58,468] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client
[2007-07-22 10:05:50,875] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client

A few lines from the log are presented in the 'Text from the log file' window. In the 'Log line/Record pattern' you need to add a pattern for the selected log. When done adding the desired pattern, click 'Verify pattern' to make sure that it was added correctly. The 'pattern verification status' will indicate whether the pattern is legal or not.

Pattern verification status
Analysis result of the log lines with the data pattern
Syntax verification - **ok**
Log analysis verification - **ok**

The 'Log records analysis result' will display a few lines from the parsed log.

Header settings – set the number of lines according the log's header length in case you wish XpoLog to disregard the log's header.

You may add a separate pattern for the header as well.

Log view settings – Check the ‘Ignore unparsed records’ if you do not want XpoLog to show you records that does not match the log’s pattern. Check the ‘Show line number’ in case you want to see the log’s line numbers (NOTE: This option will slow down XpoLog a bit).

Click next in order to move on to the last screen of the log’s wizard:

User: Admin

Modules

- Examples
 - Client
 - Server
 - MergeCS
 - Xpolog test
- Windows Event Logs
- serverlinux

Verifiers

Enterprise

Log field admin

Generated table

Date	Text 2	Priority	Text 4	Text 5	Text 6
2007-07-22 09:42:31,156	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologReports
2007-07-22 09:42:31,156	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologMaintenance
2007-07-22 09:45:05,375	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologReports

Field specification

Field Type	Field Name
1. date	Date
2. string	Text 2
3. priority	Priority
4. string	Text 4
5. string	Text 5
6. string	Text 6

Virtual columns [Add virtual column](#)

Statistics settings

☐ Compute statistics
set this option to enable statistical evaluations on this log

Indexing settings

☐ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine

[cancel](#) [previous](#) [next](#)

The third screen of the add log wizard

In this screen you can set the columns name, add a virtual column and set the statistics/indexing settings.

Rename columns – in the field name, enter the desired column name.

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.

Add Virtual Column

Operation: Merge

Columns:

- ☐ Text 2
- ☐ Priority
- ☐ Text 4
- ☐ Text 5
- ☐ Text 6

[cancel](#) [add](#)

The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.

Field specification

	Field Type	Field Name		Compute statistics:
1.	date	Date		do not compute
2.	string	Text 2		do not compute
3.	priority	Priority		do not compute
4.	string	Text 4		do not compute
5.	string	Text 5		do not compute
6.	string	Text 6		do not compute

Virtual columns [Add virtual column](#)

Statistics settings

☒ Compute statistics
set this option to enable statistical evaluations on this log

Statistical computation settings can be applied to each column separately

Indexing setting: check the ‘Use indexing’ in order to index the log. When the ‘use indexing’ is marked, a second indexing option appears:

‘Use indexing for date search’. For further information, please refer to XpoSearch.

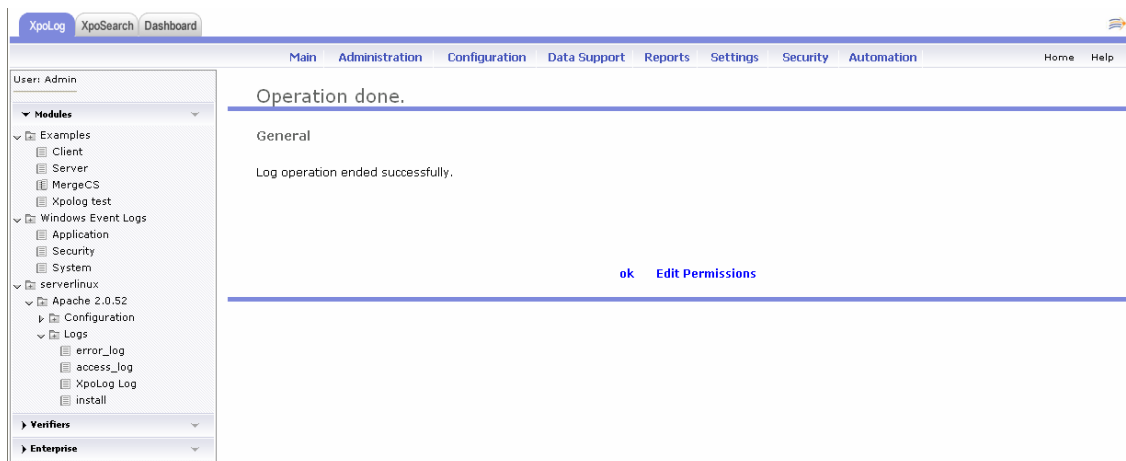
Indexing settings

☒ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine

☐ Use indexing for date search
set this option to allow for quick date search using the index

When done configuring the indexing, click ‘Next’.

The log’s wizard is done; Click OK to end the wizard. In case security is activated, you may edit the log’s permissions by clicking ‘Edit Permissions’.



5. Encrypted XML zip archive:

The screenshot shows the XpoLog configuration interface. The top navigation bar includes 'XpoLog', 'XpoSearch', and 'Dashboard'. Below this is a secondary navigation bar with 'Main', 'Administration', 'Configuration', 'Data Support', 'Reports', 'Settings', and 'Automation'. The left sidebar shows a tree view with 'Modules' (Examples, Windows Event Logs, serverlinux, serverwin, qaserver, serverdb, Test) and 'Verifiers' (Enterprise). The main content area is titled 'Log' and contains a 'General' section. This section includes fields for 'Parent module' (set to 'Examples'), 'Name', 'Description', 'Location', 'Log Path' (with a 'Browse...' button), 'Log directory path', 'File name pattern' (with an example: 'my-app-{date,dd-MM-yyyy}. {string}.log'), 'Time Zone' (set to 'Default [Asia/Jerusalem]'), 'Character Encoding' (set to 'Default'), 'Record Tag Name' (with a 'Tag name' field), and 'Encrypted Zip Password' (with a 'Password' field). At the bottom of the form are 'cancel', 'previous', and 'next' buttons.

In order to add an encrypted XML log, select the 'encrypted XML zip archive' option. Select the parent module for this log, and configure the following General data: Name, Description.

Enter the log's path and the log directory path and file name pattern will be populated automatically. You can also configure the log directory path and the log's pattern directly.

Set the logs time zone, and the character encoding.

Enter the record tag name

Click next in order to continue configuring the log.

In the second wizard's screen you will need to configure the XML log schema by specifying for each field type and name a pattern and a condition according to the XML code above. If there are missing elements or attributes please add them to the structure above and click the 'Reanalyze XML code'.

XpoLogXpoSearchDashboard

User: Admin

Modules

Examples

Client

Server

MergeCS

Xpolog test

Windows Event Logs

Application

Security

System

serverlinux

Apache 2.0.52

Configuration

Logs

error_log

access_log

XpoLog Log

install

Verifies

Enterprise

MainAdministrationConfigurationData SupportReportsSettingsSecurityAutomation

HomeHelp

XML Log schema administration

Text from the XML file

The first log element from the XML log file you specified.

```
<event logger="com.brio.one.mgmt.logging.LoggingManager" timestamp="1062802538234" level="ALWAYS" thread="Foundation Server" sequence_no="0" time="05 Sep 2003 15:55:38,234" />
<context originator_type="CommonServices" originator_name="BrioPlatform_sla1_sla1_1800" host="sla1" />
<message>*****</message>
</event>
```

reanalyze XML code

XML schema definition

Here you need to specify for each field type and name according to the XML code above

If there are missing elements or attributes please add them to the structure above and click on [reanalyze XML code](#)

Tag Name	Attribute	Value - XpoLog pattern	condition	Ignore	Tags Included
1. event		{string}	No Selected =	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2. event	logger	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
3. event	timestamp	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
4. event	level	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
5. event	thread	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
6. event	sequence_no	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
7. time		{string}		<input type="checkbox"/>	<input type="checkbox"/>
8. context		{string}	No Selected =	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9. context	originator_type	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
10. context	originator_name	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
11. context	host	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
12. message		{string}		<input type="checkbox"/>	<input type="checkbox"/>

pattern examples: {date,dd-MM-yyyy}, {number}, {string}, {priority,DEBUG;INFO;WARN;ERROR}

[pattern help](#)

Use the ‘Verify Schema’ to see a preview of the analyzed log according to the given pattern.

verify schema

Pattern verification status

Analysis result of the log lines with the data pattern

Log analysis verification - **ok**

Log records analysis result

Here you can see the log view after the xml log was analyzed the schema

logger	timestamp	level	thread	sequence_no	time	originator_type	originator_name
com.brio.one.mgmt.logging.LoggingManager	1062802538234	ALWAYS	Foundation Server	0	05 Sep 2003 15:55:38,234	CommonServices	BrioPlatform
com.brio.one.mgmt.logging.LoggingManager	1062802538265	ALWAYS	Foundation Server	1	05 Sep 2003 15:55:38,265	CommonServices	BrioPlatform
com.brio.one.mgmt.logging.LoggingManager	1062802538281	ALWAYS	Foundation Server	2	05 Sep 2003 15:55:38,281	CommonServices	BrioPlatform

cancel

previous

next

Click ‘next’ to move on to the last wizard’s screen, where you will have to configure the field specification, virtual columns, statistics computation and the use of indexing.

40

User: Admin

Modules

- Examples
 - Client
 - Server
 - MergeCS
 - Xpolog test
- Windows Event Logs
 - Application
 - Security
 - System
- serverlinux
 - Apache 2.0.52
 - Configuration
 - Logs
 - error_log
 - access_log
 - XpoLog Log
 - install

- Verifiers
- Enterprise

Log field admin

Generated table

logger	timestamp	level	thread	sequence_no	time	originator_type	originator
com.brio.one.mgmt.logging.LoggingManager	1062802538234	ALWAYS	Foundation Server	0	05 Sep 2003 15:55:38,234	CommonServices	BrioPlatf
com.brio.one.mgmt.logging.LoggingManager	1062802538265	ALWAYS	Foundation Server	1	05 Sep 2003 15:55:38,265	CommonServices	BrioPlatf
com.brio.one.mgmt.logging.LoggingManager	1062802538281	ALWAYS	Foundation Server	2	05 Sep 2003 15:55:38,281	CommonServices	BrioPlatf

Filed specification

Field Type	Field Name
1. string	logger
2. string	timestamp
3. string	level
4. string	thread
5. string	sequence_no
6. string	time
7. string	originator_type
8. string	originator_name
9. string	host
10. string	message

Virtual columns [Add virtual column](#)

Statistics settings

☐ Compute statistics
set this option to enable statistical evaluations on this log

Indexing settings

☐ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine

[cancel](#) [previous](#) [next](#)

Click 'next' in order to finish the log's wizard. You may also go back, using the 'previous' link, and reconfigure the log's properties.

6. Merge logs:

The merge logs feature allows the merge of two or more predefined logs into a single log.

User: Admin

Modules

- Examples
- Windows Event Logs
- serverlinux
 - Apache 2.0.52
 - serverwin
 - qaserver
 - serverdb
 - Test
- Verifiers
- Enterprise

Merge Logs Admin

General

Parent module:

Name:

Description:

Time Zone:

Log time zone:

Character Encoding

Character set:

Use charset according the file encoding and machine charset support.

Logs to Merge

Select the logs that will create the merged log. Only logs with date field can be merged.

☐ Modules

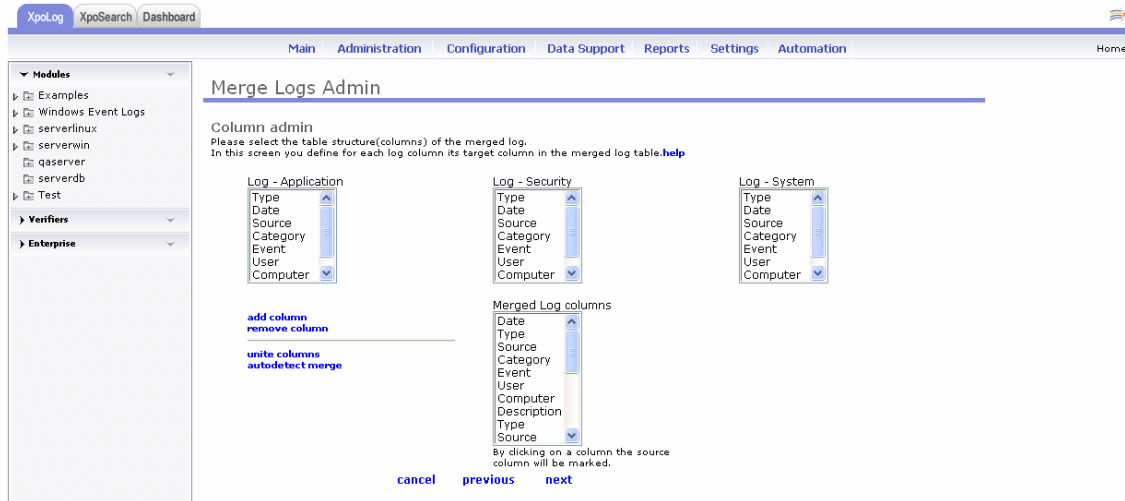
- ☐ Examples
- ☐ Windows Event Logs
 - ☐ Application
 - ☐ Security
 - ☐ System
- ☐ serverlinux
 - ☐ Apache 2.0.52
 - ☐ JBoss 4.0.0
 - ☐ Linux OS
 - ☐ Tomcat 5.5
 - ☐ Jmcat 5.0
 - ☐ WebSphere 6.1.0.0
 - ☐ serverwin
 - ☐ qaserver
 - ☐ serverdb
 - ☐ Test

[cancel](#) [previous](#) [next](#)

In the wizard, configure the general data: Parent module,

name, description, logs time zone and the character encoding.

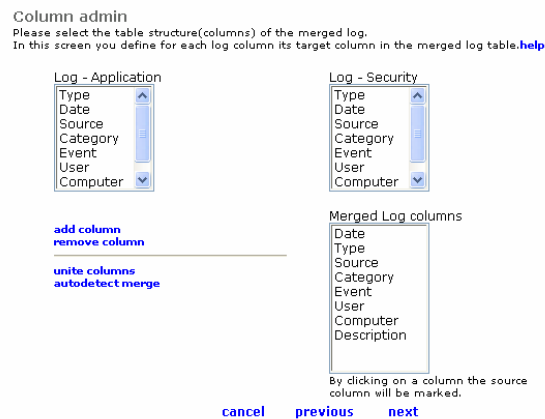
Logs to merge – Select the logs you would like to merge from the list of available logs in XpoLog, and click ‘next’.



In this screen you are configuring the merged log columns by adding columns from the source logs. XpoLog can auto detect similar columns from different source logs and unite them in the merged log.

Click the ‘Auto detect merge’ in order to activate this operation

Merge Logs Admin



The merge logs admin after auto-detection

Click ‘Next’ in order to move on to the last merge log’s configuration screen.

XpoLog XpoSearch Dashboard

Main Administration Configuration Data Support Reports Settings Automation Home

Modules

- Examples
- Windows Event Logs
- serverlinux
- serverwin
- qaserver
- serverdb
- Test
- Verifiers
- Enterprise

Merge Log field admin

Generated table

	Date	Type	Source	Category	Event	User	Computer	Description
1	05/29/2006 09:09:20	Information	SSH Tectia Server	None	0		ELNAR	Message was not found: 0 100 Server_starting
2	05/29/2006 09:09:20	Information	SSH Tectia Server	None	0		ELNAR	Message was not found: 0 105 Server_reconfig_started, File name: C:\Program Files\SSH Communication
3	05/29/2006 09:09:20	Information	SSH Tectia Server	None	0		ELNAR	Message was not found: 0 106 Server_reconfig_finished, Error: Configuration file unreadable, using defau

Filed specification

Field Type	Field Name	
1. date	Date	<input type="checkbox"/> Compute statistics on this column
2. priority	Type	<input type="checkbox"/> Compute statistics on this column
3. string	Source	<input type="checkbox"/> Compute statistics on this column
4. string	Category	<input type="checkbox"/> Compute statistics on this column
5. number	Event	<input type="checkbox"/> Compute statistics on this column
6. string	User	<input type="checkbox"/> Compute statistics on this column
7. string	Computer	<input type="checkbox"/> Compute statistics on this column
8. string	Description	<input type="checkbox"/> Compute statistics on this column

Statistics settings

☒ Compute statistics
set this option to enable statistical evaluations on this log

cancel previous next

In this screen you can see a short preview of the merged log (Generated table), and rename any of the fields name.

Moreover, you can select whether you would like XpoLog to compute statistics for the new merged log. Hence that XpoLog cannot run indexing on merged logs.

Click next, and confirm the successful creation of the merged log.

XpoLog XpoSearch Dashboard

Main Administration Configuration Data Support Reports Settings Automation Home

Modules

- Examples
- Windows Event Logs
- serverlinux
- serverwin
- qaserver
- serverdb
- Test
- Verifiers
- Enterprise

Operation done.

General

Log operation ended successfully.

ok

7. Remote XpoLogs:

Remote Log

General

Parent module: Examples

Name:

Description:

Remote Information

☒ Enterprise XpoLog Node

☐ Manual XpoLog Node

Remote Host: --Select xpolog node--

Host Address:

Protocol: HTTP

Host Port: 30303

Host Context: logeye

Security Information

☒ No login required

☐ Login with node user settings

☐ Login details

User name:

Password:

Sources

Select Source:

get log list

Please select log from remote XpoLog

save cancel

XpoLog allows you to add logs from remote XpoLogs.

Select a parent module, log name and description.

Select whether you would like to select an XpoLog node from a list of available nodes, or add one manually. A list of existing XpoLog nodes will be displayed in case such nodes were configured beforehand. For further information regarding XpoLog nodes, please refer to Data Support → Enterprise.

Remote Log

General

Parent module: Examples

Name:

Description:

Remote Information

☒ Enterprise XpoLog Node

☐ Manual XpoLog Node

Remote Host: --Select xpolog node--

Host Address:

Protocol: HTTP

Host Port: 30303

Host Context: logeye

Security Information

☒ No login required

☐ Login with node user settings

☐ Login details

User name:

Password:

Sources

Select Source:

get log list

Please select log from remote XpoLog

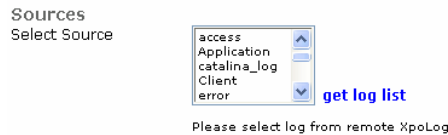
save cancel

The list of predefined XpoLog nodes

In order to manually add an XpoLog node, select 'Manual XpoLog Node' and set the host address, Protocol, and the host's port.

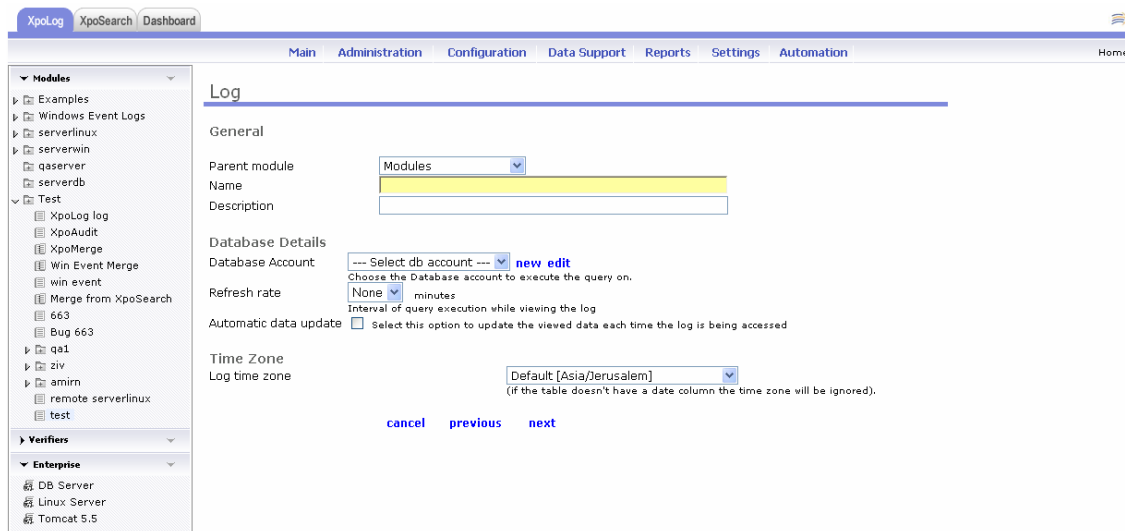
In case security is activated at the remote XpoLog node, select the ‘Login details’ and provide a valid user name and password. If the security is inactive, you can leave the ‘No login required’ option selected.

Clicking the ‘get log list’ will display all logs available in the remote XpoLog.



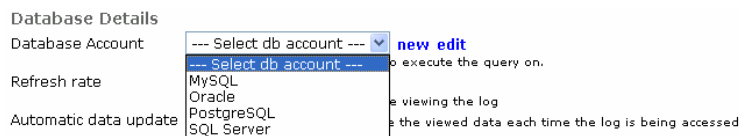
Select the log you wish to add to XpoLog and click ‘Save’.

8. Data Base query:



The database query log feature allows you to create a log based upon a DB query. In the log wizard, select a parent module, log name and description.

DB details – Select a DB account from the combo box:



Click ‘new’ in order to create a new DB account, or click ‘edit’ in order to edit an existing one. For further information on DB accounts, please refer to data support – database.

Select the ‘refresh rate’ time in minutes.

Selecting ‘Automatic data update’ will automatically update the existing data every time the log is accessed.

Click 'next' in order to continue configuring the log.

Database query administration

Database Tables List
The list of the available schemas and tables in the database you specified.

All -- Select database table --

Create Query
Here you need to specify the query you want XpoLog to execute on one or more of the tables listed above

example: SELECT * FROM TABLE1, TABLE2 [verify query](#)

Query verification status
Analysis result of the log lines with the query
Query verification - **ok**

[Show advanced Pattern Definition](#)

Log records analysis result
Here you can see the log lines after they were analyzed using the data pattern

[cancel](#) [previous](#) [next](#) [save](#)

From the database tables list select the desired schema and table available according to the DB specified.

Database query administration

Database Tables List
The list of the available schemas and tables in the database you specified.

pg_catalog pg_aggregate

Create Query
Here you need to specify the query you want XpoLog to execute on one or more of the tables listed above

SELECT * FROM pg_catalog.pg_aggregate

example: SELECT * FROM TABLE1, TABLE2 [verify query](#)

Query verification status
Analysis result of the log lines with the query
Query verification - **ok**

[Hide advanced Pattern Definition](#)

Field Name	Field Pattern
aggfnoid	{string}
aggtransfn	{string}
aggfinalfn	{string}
aggsortop	{number}
aggtranstype	{number}
agginitval	{string}

[verify patterns and query](#)

Log records analysis result
Here you can see the log lines after they were analyzed using the data pattern

	aggfnoid	aggtransfn	aggfinalfn	aggsortop	aggtranstype	agginitval
	pg_catalog.avg	int8_accum	numeric_avg	0	1231	{0,0,0}
	pg_catalog.avg	int4_avg_accum	int8_avg	0	1016	{0,0}
	pg_catalog.avg	int2_avg_accum	int8_avg	0	1016	{0,0}
	pg_catalog.avg	numeric_accum	numeric_avg	0	1231	{0,0,0}
	pg_catalog.avg	float4_accum	float8_avg	0	1022	{0,0,0}
	pg_catalog.avg	float8_accum	float8_avg	0	1022	{0,0,0}
	pg_catalog.avg	interval_accum	interval_avg	0	1187	{0 second,0 second}
	pg_catalog.sum	int8_sum	-	0	1700	
	pg_catalog.sum	int4_sum	-	0	20	
	pg_catalog.sum	int2_sum	-	0	20	

[cancel](#) [previous](#) [next](#) [save](#)

In the create query field you need to specify the query XpoLog should execute on the tables selected.

You may also change the field pattern in the advanced pattern definition. Click ‘verify query’ or ‘verify patterns and query’ to confirm it is correct. XpoLog will display a few records from the analyzed data in the ‘log records analysis’ table. Click ‘next’ in order to continue the log’s configuration or click ‘save’ if you are finished configuring.

Log field admin

Generated table

	Text 1	Text 2	Text 3	Number 4	Number 5	Text 6
pg_catalog.avg		int8_accum	numeric_avg	0	1231	{0,0,0}
pg_catalog.avg		int4_avg_accum	int8_avg	0	1016	{0,0}
pg_catalog.avg		int2_avg_accum	int8_avg	0	1016	{0,0}

Field specification

Field Type	Field Name
1. string	Text 1
2. string	Text 2
3. string	Text 3
4. number	Number 4
5. number	Number 5
6. string	Text 6

Virtual columns [Add virtual column](#)

Statistics settings

☐ Compute statistics
set this option to enable statistical evaluations on this log

Indexing settings

☐ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine

[cancel](#) [previous](#) [next](#)

‘Generated table’ is an example of how the log will look like.

In the ‘field specification’ you may change the field name of each of the columns.

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.

Add Virtual Column

Operation: Merge

Columns:

- ☐ Text 2
- ☐ Priority
- ☐ Text 4
- ☐ Text 5
- ☐ Text 6

[cancel](#) [add](#)

The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.

1.	string	Text 1	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute
2.	string	Text 2	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute
3.	string	Text 3	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute
4.	number	Number 4	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute
5.	number	Number 5	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute
6.	string	Text 6	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute

Virtual columns [Add virtual column](#)

Statistics settings
☒ Compute statistics
set this option to enable statistical evaluations on this log

Indexing settings
☒ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine
☒ Use indexing for date search
set this option to allow for quick date search using the index

Statistical computation and Indexing settings can be applied to each column separately

Indexing setting: check the ‘Use indexing’ in order to index the log.

You may select statistics computation for each and every column separately.

When the ‘use indexing’ is marked, a second indexing option appears: ‘Use indexing for date search’. For further information, please refer to XpoSearch.

Click ‘Next’ in order to finish and save the log’s wizard.

Operation done.

General

Log operation ended successfully.

[ok](#)

The log wizard ended successfully. Click ‘ok’ to confirm operation.

9. Add HTTP log configuration:

You can create an HTTP log in XpoLog. From the data source administration, select ‘Add HTTP log configuration’.

Select the parent module for this log, and specify name and description.

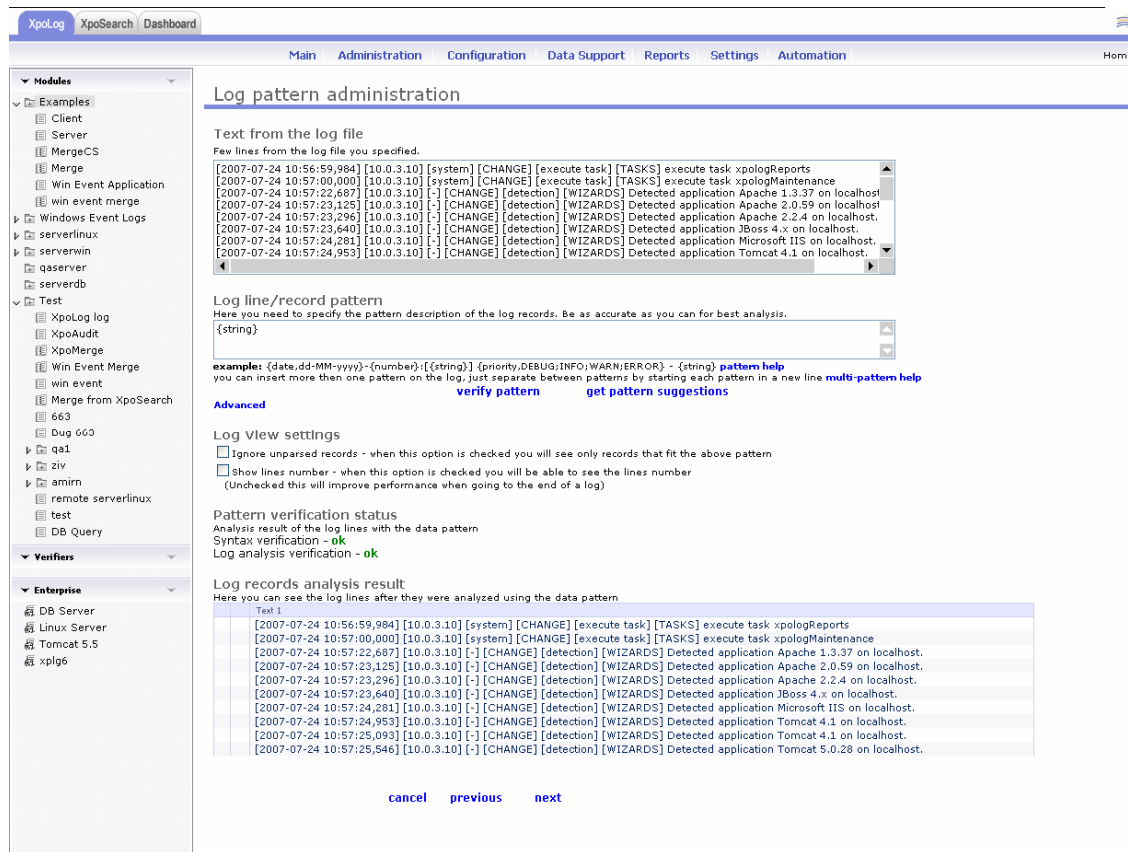
Select the relevant HTTP account for this log from the list of available accounts, or create a new HTTP account by clicking ‘new’. For further information on HTTP accounts, please refer to Data Support → Address book → HTTP.

Select the refresh rate in minutes for XpoLog to download the log file.

In the ‘file path’, you should supply the log’s relative path in the web site.

Selecting ‘Automatic data update’ will automatically update the existing data every time the log is accessed.

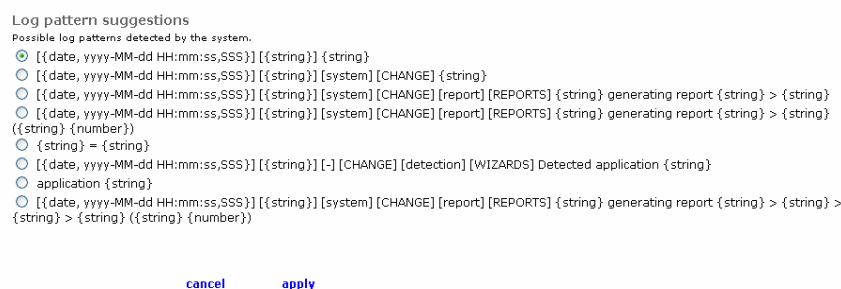
Select the log’s time zone, and click ‘next’ in order to continue the log’s configuration.



The ‘Text from the log file’ is a short preview of the log specified.

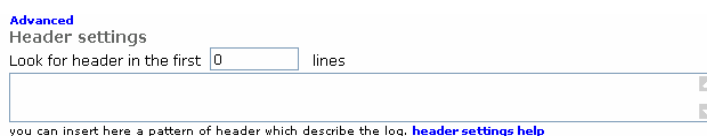
In the log line/record pattern specify a pattern according to the way you would like XpoLog to analyze the log. Click on the ‘get pattern suggestions’ and a few basic pattern alternatives to choose from, will be displayed.

Log pattern Assistant



Header settings – set the number of lines according the log’s header length in case you wish XpoLog to disregard the log’s header.

You may add a separate pattern for the header as well.



When done adding the desired pattern, click ‘Verify pattern’ to make sure that it was added correctly. The ‘pattern verification status’ will indicate whether the pattern is legal or not.

Pattern verification status
 Analysis result of the log lines with the data pattern
 Syntax verification - **ok**
 Log analysis verification - **ok**

The ‘Log records analysis result’ will display a few lines from the parsed log.

Log view settings – Check the ‘Ignore unparsed records’ if you do not want XpoLog to show you records that does not match the log’s pattern. Check the ‘Show line number’ in case you want to see the log’s line numbers (NOTE: This option will slow down XpoLog a bit).

Click next in order to move on to the last screen of the log’s wizard

The screenshot shows the 'Log field admin' screen in the XpoLog application. The interface includes a sidebar on the left with navigation options like 'Modules', 'Examples', and 'Verifiers'. The main content area is titled 'Log field admin' and contains several sections:

- Generated table:** A table showing log data with columns: Date, Text 2, Priority, Text 4, Text 5, and Text 6. The data rows show timestamps, IP addresses, and system events.
- Field specification:** A section with a table for defining field names. It lists field types (date, string, priority, string, string, string) and their corresponding field names (Date, Text 2, Priority, Text 4, Text 5, Text 6).
- Virtual columns:** A section with an 'Add virtual column' button.
- Statistics settings:** A section with a checkbox for 'Compute statistics' and a description: 'set this option to enable statistical evaluations on this log'.
- Indexing settings:** A section with a checkbox for 'Use indexing' and a description: 'using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine'.

At the bottom of the screen, there are three buttons: 'cancel', 'previous', and 'next'.

The third screen of the add log wizard

In this screen you can set the columns name, add a virtual column and set the statistics/indexing settings.

Rename columns – in the field name, enter the desired column name.

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.



The add virtual column pop up window

Check 'Compute statistics' if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.

Indexing setting: check the 'Use indexing' in order to index the log. When the 'use indexing' is marked, a second indexing option appears:

'Use indexing for date search'. For further information, please refer to XpoSearch.

Field specification

	Field Type	Field Name				
1.	date	Date	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute	▼
2.	string	Text 2	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute	▼
3.	priority	Priority	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute	▼
4.	string	Text 4	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute	▼
5.	string	Text 5	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute	▼
6.	string	Text 6	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute	▼

Virtual columns [Add virtual column](#)

Statistics settings
☒ Compute statistics
set this option to enable statistical evaluations on this log

Indexing settings
☒ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine
☒ Use indexing for date search
set this option to allow for quick date search using the index

Statistical computation and indexing settings can be applied to each column separately

When done configuring the indexing, click 'Next'.

The log's wizard is done; Click OK to end the wizard. In case security is activated, you may edit the log's permissions by clicking 'Edit Permissions'.

XpoLogXpoSearchDashboard

MainAdministrationConfigurationData SupportReportsSettingsSecurityAutomationHomeHelp

User: Admin

Modules

Examples

ClientServerMergeCSXpolog test

Windows Event Logs

ApplicationSecuritySystem

serverlinux

Apache 2.0.52

Configuration

Logs

error_logaccess_logXpoLog Loginstall

Verifiers

Enterprise

Operation done.

General

Log operation ended successfully.

okEdit Permissions

10. Add HTTP XML log configuration:

The screenshot shows the XpoLog web interface. The top navigation bar includes 'XpoLog', 'XpoSearch', and 'Dashboard'. Below this is a secondary navigation bar with links: 'Main', 'Administration', 'Configuration', 'Data Support', 'Reports', 'Settings', 'Automation', and 'Home'. The left sidebar contains a tree view with 'Modules' (Examples, Client, Server, MergeCS, Merge, Win Event Application, win event merge, HTTP, Windows Event Logs, serverlinux, serverwin, qaserver, serverdb, Test) and 'Verifiers' (Enterprise: DB Server, Linux Server, Tomcat 5.5, xplg6). The main content area is titled 'Log' and has a 'General' section with the following fields:

- Parent module:** A dropdown menu with 'Examples' selected.
- Name:** A text input field.
- Description:** A text input field.
- Http Location:**
 - Http Account:** A dropdown menu with '--- Select http account ---' and a 'new' link. Below it, a note says 'Choose the Http account from where the log file will be downloaded.'
 - Refresh rate:** A dropdown menu with 'None' selected. Below it, a note says 'When viewing the log what is the interval of downloading the log file'.
 - File path:** A text input field with an example: 'example: my-app.xml. Get more [help](#)'.
 - Automatic data update:** A checkbox labeled 'Select this option to update the viewed data each time the log is being accessed'.
- Time Zone:** A dropdown menu with 'Default [Asia/Jerusalem]' selected. Below it, a note says '(if the log doesn't have a date field the time zone will be ignored)'.
- Record Tag Name:** A text input field.

At the bottom of the 'General' section are three buttons: 'cancel', 'previous', and 'next'.

You can create an HTTP XML log in XpoLog. From the data source administration, select 'Add HTTP XML log configuration'.

Select the parent module for this log, and specify name and description.

Select the relevant HTTP account for this log from the list of available accounts, or create a new HTTP account by clicking 'new'. For further information on HTTP accounts, please refer to Data Support → Address book → HTTP.

Select the refresh rate in minutes for XpoLog to download the log file.

In the 'file path', you should supply the log's relative path in the web site.

Selecting 'Automatic data update' will automatically update the existing data every time the log is accessed. Specify the log's tag name, set the log's time zone, and click 'next' in order to continue the log's configuration.

In the second wizard's screen you will need to configure the XML log schema by specifying for each field type and name a pattern and a condition according to the XML code above. If there are missing elements or attributes please add them to the structure above and click the 'Reanalyze XML code'.

XpoLogXpoSearchDashboard

User: Admin

Modules

Examples

Client

Server

MergeCS

Xpolog test

Windows Event Logs

Application

Security

System

serverlinux

Apache 2.0.52

Configuration

Logs

error_log

access_log

XpoLog Log

install

Verifies

Enterprise

MainAdministrationConfigurationData SupportReportsSettingsSecurityAutomation

HomeHelp

XML Log schema administration

Text from the XML file

The first log element from the XML log file you specified.

```
<event logger="com.brio.one.mgmt.logging.LoggingManager" timestamp="1062802538234" level="ALWAYS" thread="Fo
<time>05 Sep 2003 15:55:38,234</time>
<context originator_type="CommonServices" originator_name="BrioPlatform_sla1_sla1_1800" host="sla1" />
<message>*****
</message>
</event>
```

reanalyze XML code

XML schema definition

Here you need to specify for each field type and name according to the XML code above

If there are missing elements or attributes please add them to the structure above and click on [reanalyze XML code](#)

Tag Name	Attribute	Value - XpoLog pattern	condition	Ignore	Tags Included
1. event		{string}	No Selected =	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2. event	logger	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
3. event	timestamp	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
4. event	level	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
5. event	thread	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
6. event	sequence_no	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
7. time		{string}		<input type="checkbox"/>	<input type="checkbox"/>
8. context		{string}	No Selected =	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9. context	originator_type	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
10. context	originator_name	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
11. context	host	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
12. message		{string}		<input type="checkbox"/>	<input type="checkbox"/>

pattern examples: {date,dd-MM-yyyy}, {number}, {string}, {priority,DEBUG;INFO;WARN;ERROR}

pattern help

Use the ‘Verify Schema’ to see a preview of the analyzed log according to the given pattern.

verify schema

Pattern verification status

Analysis result of the log lines with the data pattern

Log analysis verification - **ok**

Log records analysis result

Here you can see the log view after the xml log was analyzed the schema

	logger	timestamp	level	thread	sequence_no	time	originator_type	originator_
	com.brio.one.mgmt.logging.LoggingManager	1062802538234	ALWAYS	Foundation Server	0	05 Sep 2003 15:55:38,234	CommonServices	BrioPlatf
	com.brio.one.mgmt.logging.LoggingManager	1062802538265	ALWAYS	Foundation Server	1	05 Sep 2003 15:55:38,265	CommonServices	BrioPlatf
	com.brio.one.mgmt.logging.LoggingManager	1062802538281	ALWAYS	Foundation Server	2	05 Sep 2003 15:55:38,281	CommonServices	BrioPlatf

cancel

previous

next

Click ‘next’ to move on to the last wizard’s screen, where you will have to configure the field specification, virtual columns and statistics computation.

55

Log field admin

Generated table

	logger	timestamp	level	thread	sequence_no	time	originator_type	originator_name
	com.brio.one.mgmt.logging.LoggingManager	1062802538234	ALWAYS	Foundation Server	0	05 Sep 2003 15:55:38,234	CommonServices	BrioPlatform,
	com.brio.one.mgmt.logging.LoggingManager	1062802538265	ALWAYS	Foundation Server	1	05 Sep 2003 15:55:38,265	CommonServices	BrioPlatform,
	com.brio.one.mgmt.logging.LoggingManager	1062802538281	ALWAYS	Foundation Server	2	05 Sep 2003 15:55:38,281	CommonServices	BrioPlatform,

Filed specification

Field Type	Field Name	
1. string	logger	<input type="checkbox"/> Compute statistics on this column
2. string	timestamp	<input type="checkbox"/> Compute statistics on this column
3. string	level	<input type="checkbox"/> Compute statistics on this column
4. string	thread	<input type="checkbox"/> Compute statistics on this column
5. string	sequence_no	<input type="checkbox"/> Compute statistics on this column
6. string	time	<input type="checkbox"/> Compute statistics on this column
7. string	originator_type	<input type="checkbox"/> Compute statistics on this column
8. string	originator_name	<input type="checkbox"/> Compute statistics on this column
9. string	host	<input type="checkbox"/> Compute statistics on this column
10. string	message	<input type="checkbox"/> Compute statistics on this column

Virtual columns [Add virtual column](#)

Statistics settings
☒ Compute statistics
 set this option to enable statistical evaluations on this log

[cancel](#) [previous](#) [next](#)

Click 'next' in order to finish the log's wizard. You may also go back, using the 'previous' link, and reconfigure the log's properties.

11. Add FTP log configuration:

Log

General

Parent module: Examples

Name:

Description:

Ftp Location

Ftp Account: --- Select ftp account --- [new](#)
 Choose the Ftp account from where the log file will be downloaded.

Refresh rate: None minutes
 When viewing the log what is the interval of downloading the log file

File path:
 The relative location for the log on the web site

File name pattern:
 example: my-app-{date,dd-MM-yyyy}-{string}.log. Get more [help](#)

Automatic data update: ☐ Select this option to update the viewed data each time the log is being accessed

Time Zone: Default [Asia/Jerusalem]
 Log time zone: (if the log doesn't have a date field the time zone will be ignored).

[cancel](#) [previous](#) [next](#)

In order to create an FTP log in XpoLog, from the data source administration, select 'Add FTP log configuration'.

Select the parent module for this log, and specify name and description.

Select the relevant FTP account for this log from the list of available accounts, or create a new FTP account by clicking 'new'. For further

information on FTP accounts, please refer to Data Support → Address book → FTP.

Select the refresh rate in minutes for XpoLog to download the log file.

In the ‘file path’, you should supply the log’s relative path in the web site.

Selecting ‘Automatic data update’ will automatically update the existing data every time the log is accessed.

Select the log’s time zone, and click ‘next’ in order to continue the log’s configuration.

Log pattern administration

Text from the log file

Few lines from the log file you specified.

```
[2007-07-24 10:56:59,984] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-24 10:57:00,000] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-24 10:57:22,687] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Apache 1.3.37 on localhost.
[2007-07-24 10:57:23,125] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Apache 2.0.59 on localhost.
[2007-07-24 10:57:23,296] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Apache 2.2.4 on localhost.
[2007-07-24 10:57:23,640] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application JBoss 4.x on localhost.
[2007-07-24 10:57:24,281] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Microsoft IIS on localhost.
[2007-07-24 10:57:24,953] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Tomcat 4.1 on localhost.
```

Log line/record pattern

Here you need to specify the pattern description of the log records. Be as accurate as you can for best analysis.

{string}

example: {date,dd-MM-yyyy}-{number}-{string}-{priority,DEBUG;INFO;WARN;ERROR} - {string} [pattern help](#)

you can insert more then one pattern on the log, just separate between patterns by starting each pattern in a new line [multi-pattern help](#)

[verify pattern](#) [get pattern suggestions](#)

Advanced

Header settings

Look for header in the first lines

you can insert here a pattern of header which describe the log. [header settings help](#)

Log View settings

☐ Ignore unparsed records - when this option is checked you will see only records that fit the above pattern

☐ Show lines number - when this option is checked you will be able to see the lines number
(Unchecked this will improve performance when going to the end of a log)

Pattern verification status

Analysis result of the log lines with the data pattern

Syntax verification - **ok**

Log analysis verification - **ok**

Log records analysis result

Here you can see the log lines after they were analyzed using the data pattern

Text 1
[2007-07-24 10:56:59,984] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-24 10:57:00,000] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-24 10:57:22,687] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Apache 1.3.37 on localhost.
[2007-07-24 10:57:23,125] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Apache 2.0.59 on localhost.
[2007-07-24 10:57:23,296] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Apache 2.2.4 on localhost.
[2007-07-24 10:57:23,640] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application JBoss 4.x on localhost.
[2007-07-24 10:57:24,281] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Microsoft IIS on localhost.
[2007-07-24 10:57:24,953] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Tomcat 4.1 on localhost.
[2007-07-24 10:57:25,093] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Tomcat 4.1 on localhost.
[2007-07-24 10:57:25,546] [10.0.3.10] [-] [CHANGE] [detection] [WIZARDS] Detected application Tomcat 5.0.28 on localhost.

The ‘Text from the log file’ is a short preview of the log specified.

In the log line/record pattern specify a pattern according to the way you would like XpoLog to analyze the log. Click on the ‘get pattern suggestions’ and a few basic pattern alternatives to choose from, will be displayed.

Log pattern Assistant

Log pattern suggestions

Possible log patterns detected by the system.

- ☒ `{{date, yyyy-MM-dd HH:mm:ss,SSS}} [{{string}}] {string}`
- ☐ `{{date, yyyy-MM-dd HH:mm:ss,SSS}} [{{string}}] [system] [CHANGE] {string}`
- ☐ `{{date, yyyy-MM-dd HH:mm:ss,SSS}} [{{string}}] [system] [CHANGE] [report] [REPORTS] {string} generating report {string} > {string}`
- ☐ `{{date, yyyy-MM-dd HH:mm:ss,SSS}} [{{string}}] [system] [CHANGE] [report] [REPORTS] {string} generating report {string} > {string} {string} {number}`
- ☐ `{string} = {string}`
- ☐ `{{date, yyyy-MM-dd HH:mm:ss,SSS}} [{{string}}] [-] [CHANGE] [detection] [WIZARDS] Detected application {string}`
- ☐ `application {string}`
- ☐ `{{date, yyyy-MM-dd HH:mm:ss,SSS}} [{{string}}] [system] [CHANGE] [report] [REPORTS] {string} generating report {string} > {string} > {string} > {string} {string} {number}`

[cancel](#) [apply](#)

Header settings – set the number of lines according the log’s header length in case you wish XpoLog to disregard the log’s header.

You may add a separate pattern for the header as well.

Advanced
Header settings
Look for header in the first lines

you can insert here a pattern of header which describe the log. [header settings help](#)

When done adding the desired pattern, click ‘Verify pattern’ to make sure that it was added correctly. The ‘pattern verification status’ will indicate whether the pattern is legal or not.

Pattern verification status

Analysis result of the log lines with the data pattern

Syntax verification - **ok**

Log analysis verification - **ok**

The ‘Log records analysis result’ will display a few lines from the parsed log.

Log view settings – Check the ‘Ignore unparsed records’ if you do not want XpoLog to show you records that does not match the log’s pattern. Check the ‘Show line number’ in case you want to see the log’s line numbers (NOTE: This option will slow down XpoLog a bit).

Click next in order to move on to the last screen of the log’s wizard

User: Admin

Modules

- Examples
 - Client
 - Server
 - MergeCS
 - Xpolog test
- Windows Event Logs
- serverlinux

Verifiers

- Enterprise

Log field admin

Generated table

Date	Text 2	Priority	Text 4	Text 5	Text 6
2007-07-22 09:42:31,156	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologReports
2007-07-22 09:42:31,156	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologMaintenance
2007-07-22 09:45:05,375	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologReports

Field specification

Field Type	Field Name
1. date	Date
2. string	Text 2
3. priority	Priority
4. string	Text 4
5. string	Text 5
6. string	Text 6

Virtual columns [Add virtual column](#)

Statistics settings

☐ Compute statistics
set this option to enable statistical evaluations on this log

Indexing settings

☐ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine

[cancel](#) [previous](#) [next](#)

The third screen of the add log wizard

In this screen you can set the columns name, add a virtual column and set the statistics/indexing settings.

Rename columns – in the field name, enter the desired column name.

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.

Add Virtual Column

Operation: Merge

Columns:

- Text 2
- Priority
- Text 4
- Text 5
- Text 6

[cancel](#) [add](#)

The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.

Indexing setting: check the ‘Use indexing’ in order to index the log. When the ‘use indexing’ is marked, a second indexing option appears:

‘Use indexing for date search’. For further information, please refer to XpoSearch.

Field specification

	Field Type	Field Name				
1.	date	Date	<input checked="" type="checkbox"/>	Index this column	Compute statistics:	do not compute
2.	string	Text 2	<input checked="" type="checkbox"/>	Index this column	Compute statistics:	do not compute
3.	priority	Priority	<input checked="" type="checkbox"/>	Index this column	Compute statistics:	do not compute
4.	string	Text 4	<input checked="" type="checkbox"/>	Index this column	Compute statistics:	do not compute
5.	string	Text 5	<input checked="" type="checkbox"/>	Index this column	Compute statistics:	do not compute
6.	string	Text 6	<input checked="" type="checkbox"/>	Index this column	Compute statistics:	do not compute

Virtual columns [Add virtual column](#)

Statistics settings

☒ Compute statistics
set this option to enable statistical evaluations on this log

Indexing settings

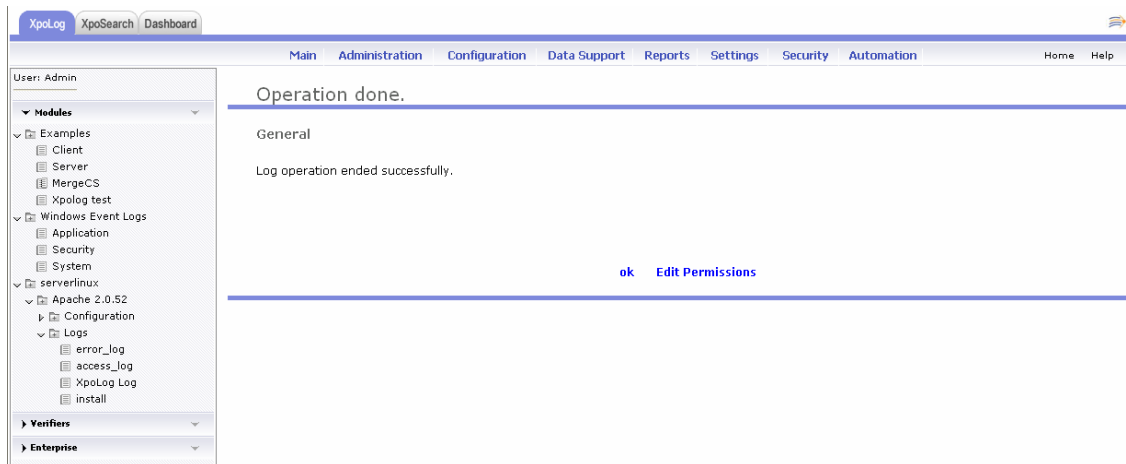
☒ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine

☒ Use indexing for date search
set this option to allow for quick date search using the index

Statistical computation and indexing settings can be applied to each column separately

When done configuring the indexing, click 'Next'.

The log's wizard is done; Click OK to end the wizard. In case security is activated, you may edit the log's permissions by clicking 'Edit Permissions'.



12. Add FTP XML log configuration:

The screenshot shows the XpoLog 'Log' configuration wizard. The sidebar on the left contains a tree view of modules, including Apache, JBoss, IIS, Tomcat, Windows Event Logs, serverlinux, 10.0.0.9, 10.0.0.20, Examples, serverwin, qaserver, serverdb, and Test. The main configuration area is titled 'Log' and contains the following sections:

- General**
 - Parent module: default
 - Name: [text input]
 - Description: [text input]
- Ftp Location**
 - Ftp Account: [dropdown menu] new
 - Refresh rate: None
 - File path: [text input] example: my-app.xml. Get more help
 - File name pattern: [text input] example: my-app-{date,dd-MM-yyyy}-{string}.log. Get more help
 - Automatic data update: ☐ Select this option to update the viewed data each time the log is being accessed
- Time Zone**
 - Log time zone: Default [Asia/Jerusalem]
- Record Tag Name**
 - Tag name: [text input]

At the bottom of the configuration area are three buttons: cancel, previous, and next.

You can create an FTP XML log in XpoLog. From the data source administration, select 'Add FTP XML log configuration'.

Select the parent module for this log, and specify name and description.

Select the relevant FTP account for this log from the list of available accounts, or create a new FTP account by clicking 'new'. For further information on FTP accounts, please refer to Data Support → Address book → FTP.

Select the refresh rate in minutes for XpoLog to download the log file.

In the 'file path', you should supply the log's relative path in the web site.

Selecting 'Automatic data update' will automatically update the existing data every time the log is accessed. Specify the log's tag name, set the log's time zone, and click 'next' in order to continue the log's configuration.

In the second wizard's screen you will need to configure the XML log schema by specifying for each field type and name a pattern and a condition according to the XML code above. If there are missing elements or attributes please add them to the structure above and click the 'Reanalyze XML code'.

XpoLogXpoSearchDashboard

User: Admin

Modules

Examples

Client

Server

MergeCS

Xpolog test

Windows Event Logs

Application

Security

System

serverlinux

Apache 2.0.52

Configuration

Logs

error_log

access_log

XpoLog Log

install

Verifies

Enterprise

MainAdministrationConfigurationData SupportReportsSettingsSecurityAutomation

HomeHelp

XML Log schema administration

Text from the XML file

The first log element from the XML log file you specified.

```
<event logger="com.brio.one.mgmt.logging.LoggingManager" timestamp="1062802538234" level="ALWAYS" thread="Fo
<time>05 Sep 2003 15:55:38,234</time>
<context originator_type="CommonServices" originator_name="BrioPlatform_sla1_sla1_1800" host="sla1" />
<message>*****</message>
</event>
```

reanalyze XML code

XML schema definition

Here you need to specify for each field type and name according to the XML code above

If there are missing elements or attributes please add them to the structure above and click on [reanalyze XML code](#)

Tag Name	Attribute	Value - XpoLog pattern	condition	Ignore	Tags Included
1. event		{string}	No Selected =	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2. event	logger	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
3. event	timestamp	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
4. event	level	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
5. event	thread	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
6. event	sequence_no	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
7. time		{string}		<input type="checkbox"/>	<input type="checkbox"/>
8. context		{string}	No Selected =	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9. context	originator_type	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
10. context	originator_name	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
11. context	host	{string}	No Selected =	<input type="checkbox"/>	<input type="checkbox"/>
12. message		{string}		<input type="checkbox"/>	<input type="checkbox"/>

pattern examples: {date,dd-MM-yyyy}, {number}, {string}, {priority,DEBUG;INFO;WARN;ERROR}

pattern help

Use the ‘Verify Schema’ to see a preview of the analyzed log according to the given pattern.

verify schema

Pattern verification status

Analysis result of the log lines with the data pattern

Log analysis verification - **ok**

Log records analysis result

Here you can see the log view after the xml log was analyzed the schema

logger	timestamp	level	thread	sequence_no	time	originator_type	originator_name
com.brio.one.mgmt.logging.LoggingManager	1062802538234	ALWAYS	Foundation Server	0	05 Sep 2003 15:55:38,234	CommonServices	BrioPlatform
com.brio.one.mgmt.logging.LoggingManager	1062802538265	ALWAYS	Foundation Server	1	05 Sep 2003 15:55:38,265	CommonServices	BrioPlatform
com.brio.one.mgmt.logging.LoggingManager	1062802538281	ALWAYS	Foundation Server	2	05 Sep 2003 15:55:38,281	CommonServices	BrioPlatform

cancel

previous

next

Click ‘next’ to move on to the last wizard’s screen, where you will have to configure the field specification, virtual columns and statistics computation.

62

Log field admin

Generated table

logger	timestamp	level	thread	sequence_no	time	originator_type	originator_name
com.brio.one.mgmt.logging.LoggingManager	1062802538234	ALWAYS	Foundation Server	0	05 Sep 2003 15:55:38,234	CommonServices	BrioPlatform,
com.brio.one.mgmt.logging.LoggingManager	1062802538265	ALWAYS	Foundation Server	1	05 Sep 2003 15:55:38,265	CommonServices	BrioPlatform,
com.brio.one.mgmt.logging.LoggingManager	1062802538281	ALWAYS	Foundation Server	2	05 Sep 2003 15:55:38,281	CommonServices	BrioPlatform,

Filed specification

Field Type	Field Name	Compute statistics on this column
1. string	logger	<input type="checkbox"/>
2. string	timestamp	<input type="checkbox"/>
3. string	level	<input type="checkbox"/>
4. string	thread	<input type="checkbox"/>
5. string	sequence_no	<input type="checkbox"/>
6. string	time	<input type="checkbox"/>
7. string	originator_type	<input type="checkbox"/>
8. string	originator_name	<input type="checkbox"/>
9. string	host	<input type="checkbox"/>
10. string	message	<input type="checkbox"/>

Virtual columns [Add virtual column](#)

Statistics settings
☒ Compute statistics
 set this option to enable statistical evaluations on this log

[cancel](#) [previous](#) [next](#)

Click 'next' in order to finish the log's wizard. You may also go back, using the 'previous' link, and reconfigure the log's properties.

13. Add SSH log configuration:

Log

General

Parent module: default

Name:

Description:

SSH Location

SSH Account: --- Select ssh account --- [new](#)

Choose the SSH account from where the log file will be processed.

File path:

The relative location for the log on the web site

File name pattern:

example: my-app-{date,dd-MM-yyyy}-{string}.log. [Get more help](#)

Advanced

Data Access Mode

☒ Online Access files remotely using SSH

☐ Offline Download files

Automatic update ☐ Select this option to update the viewed data each time the log is being accessed

When viewing the log what is the interval of downloading the log file

Refresh rate: None minutes

Time Zone

Log time zone: Default [Asia/Jerusalem]

(if the log doesn't have a date field the time zone will be ignored).

Character Encoding

Character set: Default

Use charset according the file encoding and machine charset support.

[cancel](#) [previous](#) [next](#)

In order to create an SSH log in XpoLog, from the data source administration, select 'Add SSH log configuration'.

Select the parent module for this log, and specify name and description.

Select the relevant SSH account for this log from the list of available

accounts, or create a new SSH account by clicking ‘new’. For further information on SSH accounts, please refer to Data Support → Address book → SSH.

Specify the log’s relative path in the ‘file path’, and the file name pattern for the log files.

Data access mode – The files can be accessed both online or offline. Select ‘online’ in order to access the files remotely, using SSH. Select ‘offline’ in order to download the log’s files. If the offline option was selected, you may set the automatic update option – in order to auto-update the data every time the log is accessed, or you may set a refresh rate in minutes instead.

Select the log’s time zone, and encoding. When done, click ‘next’ in order to continue to the wizard’s next screen.

The next wizard screen is the log pattern administration:

User: Admin

Modules Verifiers Enterprise

Main Administration Configuration Data Support Reports Settings Security Automation Home Help

Log pattern administration

Text from the log file

Few lines from the log file you specified.

```
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:45:05,375] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:45:05,390] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:57:18,187] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task SearchEngineIntervalIndex
[2007-07-22 10:00:00,031] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task XpoLogRemoteSessionMain
```

Log line/record pattern

Here you need to specify the pattern description of the log records. Be as accurate as you can for best analysis.

{string}

example: {date,dd-MM-yyyy}-{number}-{(string)} {priority,DEBUG;INFO;WARN;ERROR} - {string} [pattern help](#)
you can insert more than one pattern on the log, just separate between patterns by starting each pattern in a new line [multi-pattern help](#)

[verify pattern](#) [get pattern suggestions](#)

Advanced

Header settings

Look for header in the first lines

you can insert here a pattern of header which describe the log. [header settings help](#)

Log View settings

☐ Ignore unparsed records - when this option is checked you will see only records that fit the above pattern

☐ Show lines number - when this option is checked you will be able to see the lines number
(Unchecked this will improve performance when going to the end of a log)

Pattern verification status

Analysis result of the log lines with the data pattern

Syntax verification - **ok**

Log analysis verification - **ok**

Log records analysis result

Here you can see the log lines after they were analyzed using the data pattern

Text
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:42:31,156] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:45:05,375] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologReports
[2007-07-22 09:45:05,390] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 09:57:18,187] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task xpologMaintenance
[2007-07-22 10:00:00,015] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task SearchEngineIntervalIndex
[2007-07-22 10:00:00,031] [10.0.3.10] [system] [CHANGE] [execute task] [TASKS] execute task XpoLogRemoteSessionMaintenance
[2007-07-22 10:00:00,031] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client
[2007-07-22 10:05:50,875] [10.0.3.10] [-] [VIEW] [log view] [LOGS] view the log Client

The second screen of the add log wizard

A few lines from the log are presented in the ‘Text from the log file’ window. In the ‘Log line/Record pattern’ you need to add a pattern for the

selected log. When done adding the desired pattern, click ‘Verify pattern’ to make sure that it was added correctly. The ‘pattern verification status’ will indicate whether the pattern is legal or not.

Pattern verification status
 Analysis result of the log lines with the data pattern
 Syntax verification - **ok**
 Log analysis verification - **ok**

The ‘Log records analysis result’ will display a few lines from the parsed log.

Header settings – set the number of lines according the log’s header length in case you wish XpoLog to disregard the log’s header.

You may add a separate pattern for the header as well.

Log view settings – Check the ‘Ignore unparsed records’ if you do not want XpoLog to show you records that does not match the log’s pattern. Check the ‘Show line number’ in case you want to see the log’s line numbers (NOTE: This option will slow down XpoLog a bit).

Click next in order to move on to the last screen of the log’s wizard:

User: Admin

Modules

- Examples
 - Client
 - Server
 - MergeCS
 - Xpolog test
- Windows Event Logs
- serverlinux
- Verifiers
- Enterprise

Log field admin

Generated table

Date	Text 2	Priority	Text 4	Text 5	Text 6
2007-07-22 09:42:31,156	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologReports
2007-07-22 09:42:31,156	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologMaintenance
2007-07-22 09:45:05,375	10.0.3.10	system	CHANGE	execute task	[TASKS] execute task xpologReports

Field specification

Field Type	Field Name
1. date	Date
2. string	Text 2
3. priority	Priority
4. string	Text 4
5. string	Text 5
6. string	Text 6

Virtual columns [Add virtual column](#)

Statistics settings

☐ Compute statistics
 set this option to enable statistical evaluations on this log

Indexing settings

☐ Use indexing
 using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine

[cancel](#) [previous](#) [next](#)

The third screen of the add log wizard

In this screen you can set the columns name, add a virtual column and set the statistics/indexing settings.

Rename columns – in the field name, enter the desired column name.

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.



The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.

Indexing setting: check the ‘Use indexing’ in order to index the log. When the ‘use indexing’ is marked, a second indexing option appears:

‘Use indexing for date search’. For further information, please refer to XpoSearch.

Field specification

Field Type	Field Name			
1. date	Date	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute
2. string	Text 2	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute
3. priority	Priority	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute
4. string	Text 4	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute
5. string	Text 5	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute
6. string	Text 6	<input checked="" type="checkbox"/> Index this column	Compute statistics:	do not compute

Virtual columns [Add virtual column](#)

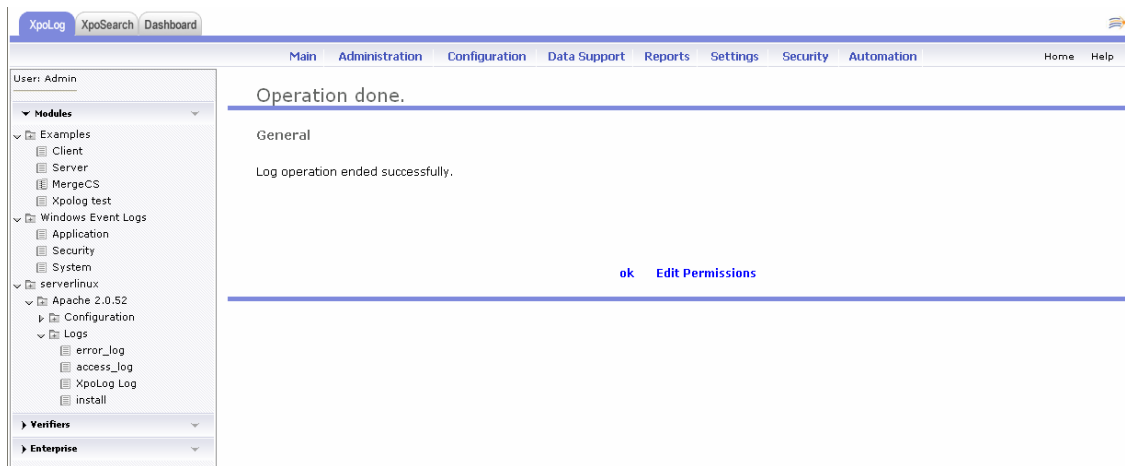
Statistics settings
☒ Compute statistics
set this option to enable statistical evaluations on this log

Indexing settings
☒ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine
☒ Use indexing for date search
set this option to allow for quick date search using the index

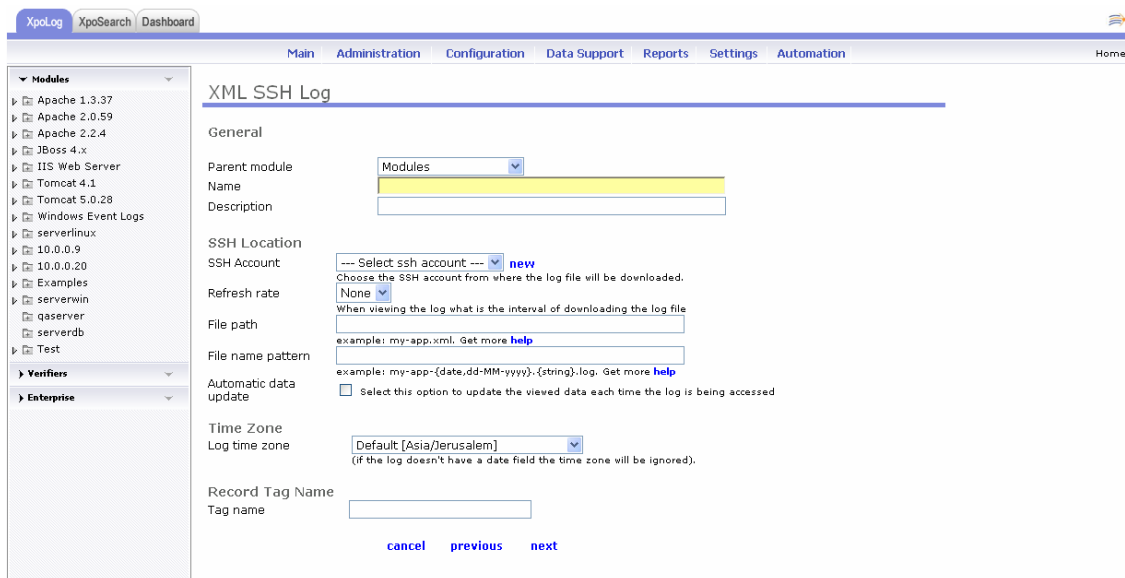
Statistical computation and indexing settings can be applied to each column separately

When done configuring the indexing, click ‘Next’.

The log’s wizard is done; Click OK to end the wizard. In case security is activated, you may edit the log’s permissions by clicking ‘Edit Permissions’.



14. Add SSH XML log configuration:



It is possible to create an SSH XML log in XpoLog. From the data source administration, select 'Add SSH XML log configuration'.

Select the parent module for this log, and specify a name and description.

Select the relevant SSH account for this log from the list of available accounts, or create a new SSH account by clicking 'new'. For further information on SSH accounts, please refer to Data Support → Address book → SSH.

Select the refresh rate in minutes for XpoLog to download the log file.

In the 'file path', you should supply the log's relative path in the web site followed by its name pattern. Selecting 'Automatic data update' will

automatically update the existing data every time the log is accessed.

Specify the log's tag name, set the log's time zone, and click 'next' in order to continue the log's configuration.

In the second wizard's screen you will need to configure the XML log schema by specifying for each field type and name a pattern and a condition according to the XML code above. If there are missing elements or attributes please add them to the structure above and click the 'Reanalyze XML code'.

XML Log schema administration

Text from the XML file

The first log element from the XML log file you specified.

```
<event logger="com.brio.one.mgmt.logging.LoggingManager" timestamp="1062802538234" level="ALWAYS" thread="Fr">
  <time>05 Sep 2003 15:55:38,234</time>
  <context originator_type="CommonServices" originator_name="BrioPlatform_sla1_sla1_1800" host="sla1" />
  <message>*****</message>
</event>
```

reanalyze XML code

XML schema definition

Here you need to specify for each field type and name according to the XML code above. If there are missing elements or attributes please add them to the structure above and click on [reanalyze XML code](#)

Tag Name	Attribute	Value - XpoLog pattern	condition	Ignore	Tags Included
1. event		{string}	No Selected	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2. event	logger	{string}	No Selected	<input type="checkbox"/>	<input type="checkbox"/>
3. event	timestamp	{string}	No Selected	<input type="checkbox"/>	<input type="checkbox"/>
4. event	level	{string}	No Selected	<input type="checkbox"/>	<input type="checkbox"/>
5. event	thread	{string}	No Selected	<input type="checkbox"/>	<input type="checkbox"/>
6. event	sequence_no	{string}	No Selected	<input type="checkbox"/>	<input type="checkbox"/>
7. time		{string}		<input type="checkbox"/>	<input type="checkbox"/>
8. context		{string}	No Selected	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9. context	originator_type	{string}	No Selected	<input type="checkbox"/>	<input type="checkbox"/>
10. context	originator_name	{string}	No Selected	<input type="checkbox"/>	<input type="checkbox"/>
11. context	host	{string}	No Selected	<input type="checkbox"/>	<input type="checkbox"/>
12. message		{string}		<input type="checkbox"/>	<input type="checkbox"/>

pattern examples: {date,dd-MM-yyyy}, {number}, {string}, {priority,DEBUG;INFO;WARN;ERROR} [pattern help](#)

Use the 'Verify Schema' to see a preview of the analyzed log according to the given pattern.

verify schema

Pattern verification status

Analysis result of the log lines with the data pattern

Log analysis verification - **ok**

Log records analysis result

Here you can see the log view after the xml log was analyzed the schema

logger	timestamp	level	thread	sequence_no	time	originator_type	originator_name
com.brio.one.mgmt.logging.LoggingManager	1062802538234	ALWAYS	Foundation Server	0	05 Sep 2003 15:55:38,234	CommonServices	BrioPlatform
com.brio.one.mgmt.logging.LoggingManager	1062802538265	ALWAYS	Foundation Server	1	05 Sep 2003 15:55:38,265	CommonServices	BrioPlatform
com.brio.one.mgmt.logging.LoggingManager	1062802538281	ALWAYS	Foundation Server	2	05 Sep 2003 15:55:38,281	CommonServices	BrioPlatform

cancel previous next

Click ‘next’ to move on to the last wizard’s screen, where you will have to configure the field specification, virtual columns and statistics computation.

Log field admin

Generated table

logger	timestamp	level	thread	sequence_no	time	originator_type	originator_name
com.brio.one.mgmt.logging.LoggingManager	1062802538234	ALWAYS	Foundation Server	0	05 Sep 2003 15:55:38,234	CommonServices	BrioPlatform
com.brio.one.mgmt.logging.LoggingManager	1062802538265	ALWAYS	Foundation Server	1	05 Sep 2003 15:55:38,265	CommonServices	BrioPlatform
com.brio.one.mgmt.logging.LoggingManager	1062802538281	ALWAYS	Foundation Server	2	05 Sep 2003 15:55:38,281	CommonServices	BrioPlatform

Filed specification

Field Type	Field Name	Compute statistics on this column
1. string	logger	<input type="checkbox"/>
2. string	timestamp	<input type="checkbox"/>
3. string	level	<input type="checkbox"/>
4. string	thread	<input type="checkbox"/>
5. string	sequence_no	<input type="checkbox"/>
6. string	time	<input type="checkbox"/>
7. string	originator_type	<input type="checkbox"/>
8. string	originator_name	<input type="checkbox"/>
9. string	host	<input type="checkbox"/>
10. string	message	<input type="checkbox"/>

Virtual columns [Add virtual column](#)

Statistics settings
☒ Compute statistics
 set this option to enable statistical evaluations on this log

[cancel](#) [previous](#) [next](#)

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.

Add Virtual Column

Operation: Merge

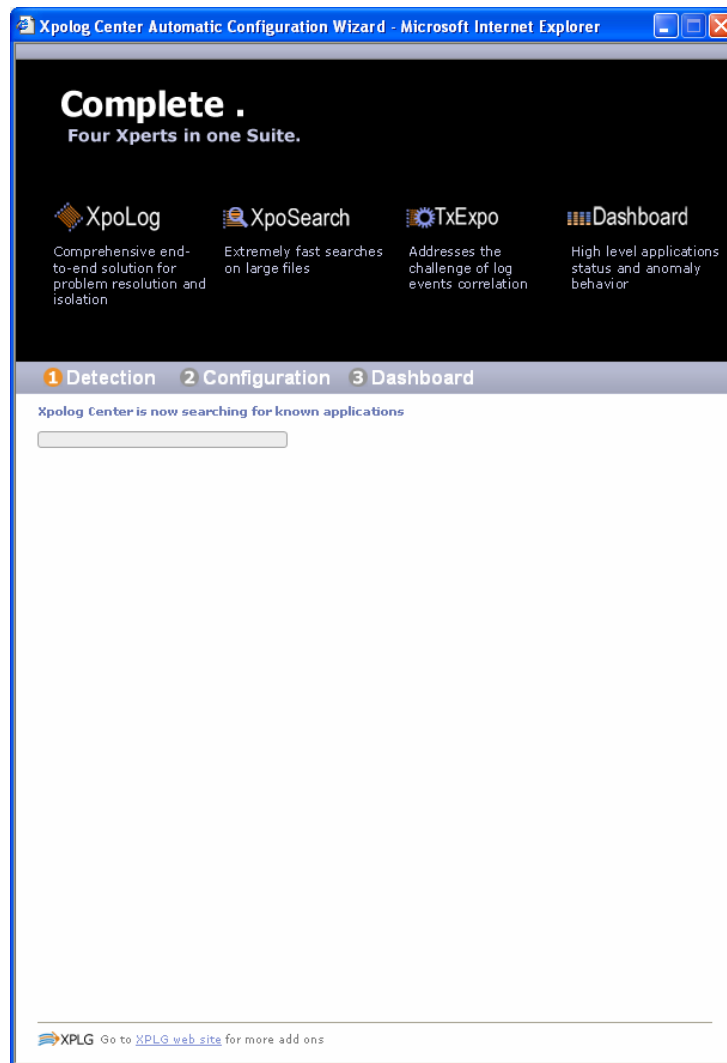
Columns: logger, timestamp, level, thread, sequence_no

[cancel](#) [add](#)

The add virtual column pop up window

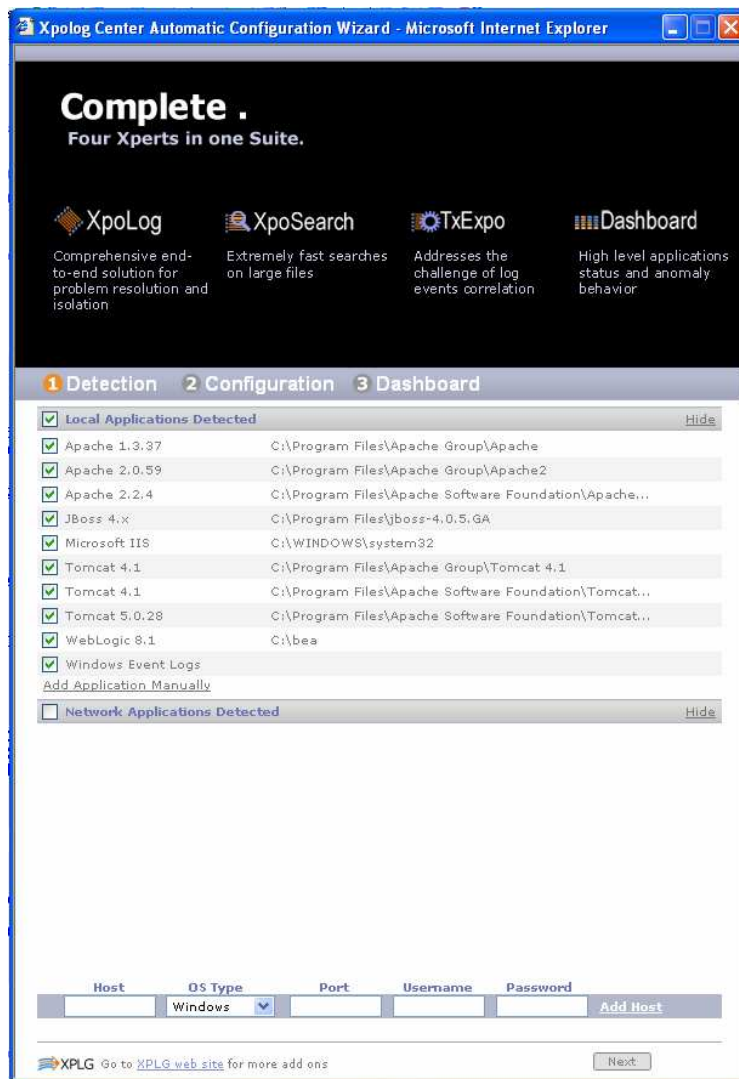
Click ‘next’ in order to finish the log’s wizard. You may also go back, using the ‘previous’ link, and reconfigure the log’s properties.

15. Automatic configuration wizard:



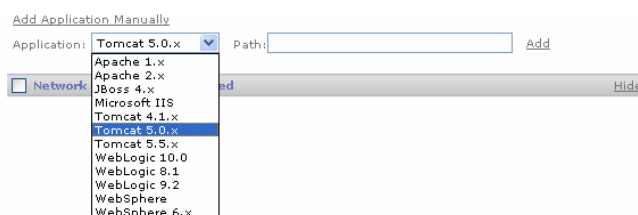
The automatic configuration wizard allows you to automatically detect and add logs from a list of known applications to XpoLog.

Click the 'Run automatic configuration wizard' in Administration → add log. In the first stage, the automatic detection processes will search for known application installed on your local machine, displaying available results.



At this stage, select all desired applications found on your local machine in order to add them to XpoLog.

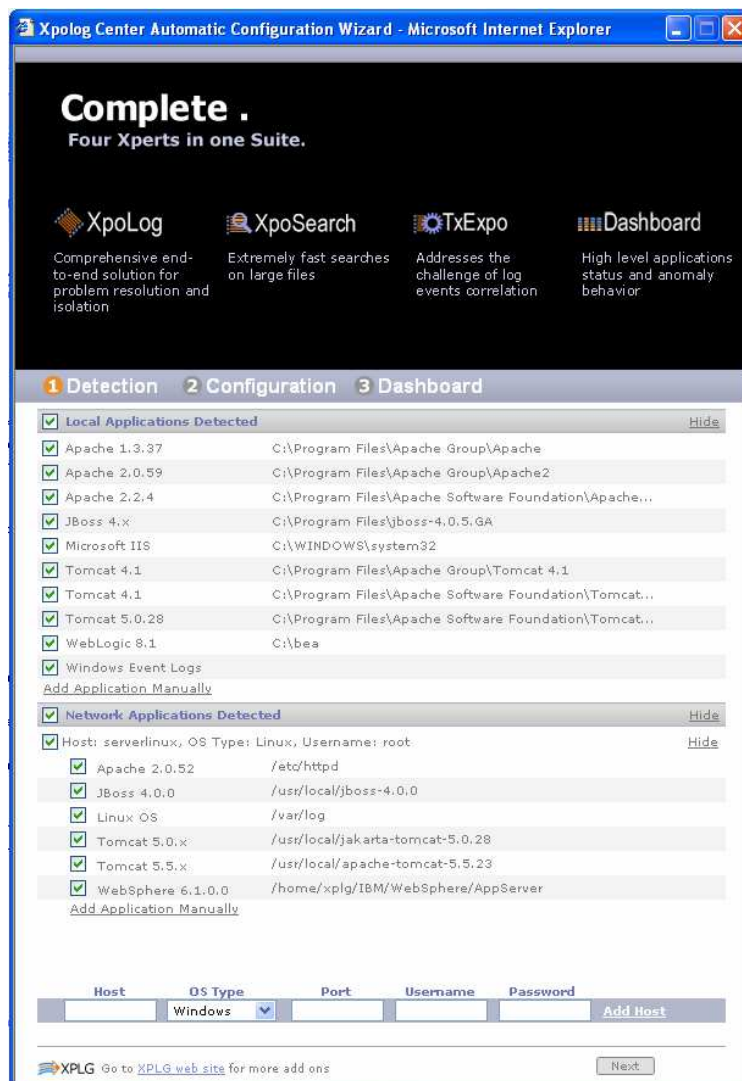
In case there is an application (On local machine) that the automatic wizard did not detect you may do so manually. Click the ‘add application manually’, select the application type from the list of available applications, specify it’s path, and click add.



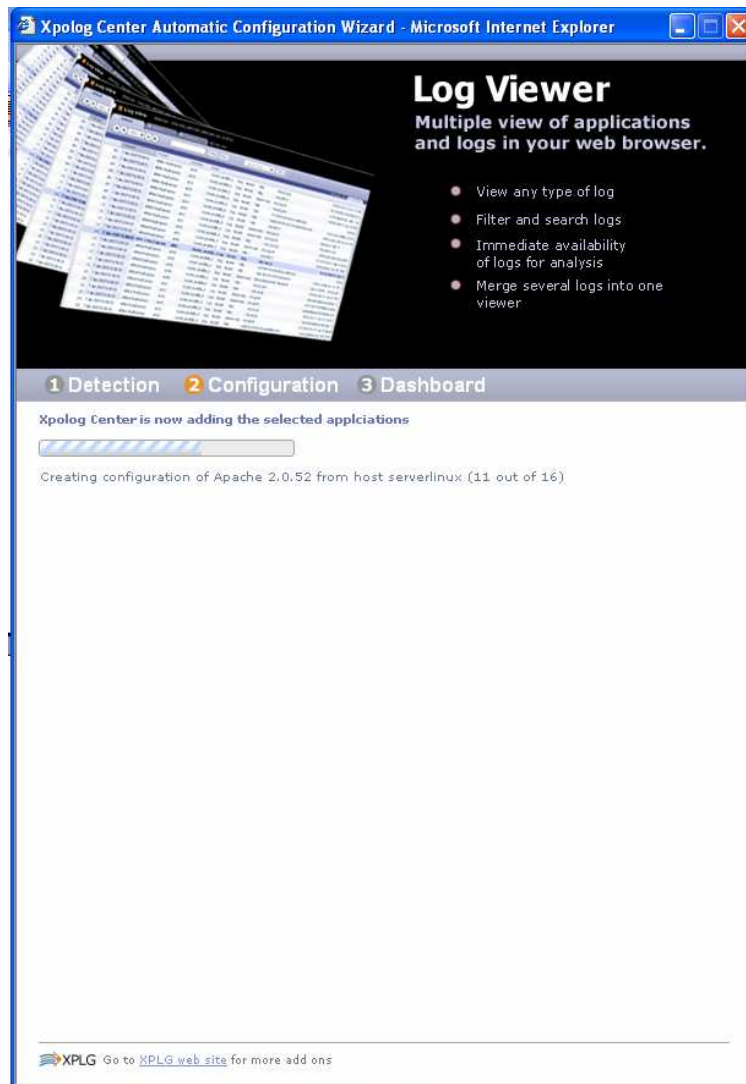
Network applications - The automatic detection wizard can add known applications' logs, located on remote machines in your network to XpoLog as well. Specify a host name for the machine that hosts the logs you wish to add, select the host's operating system, the connection port and a username and password. Click 'Add host'

The automatic detection wizard will search for known applications and add all available logs. You can add applications manually from the network, in a similar way as in local applications.

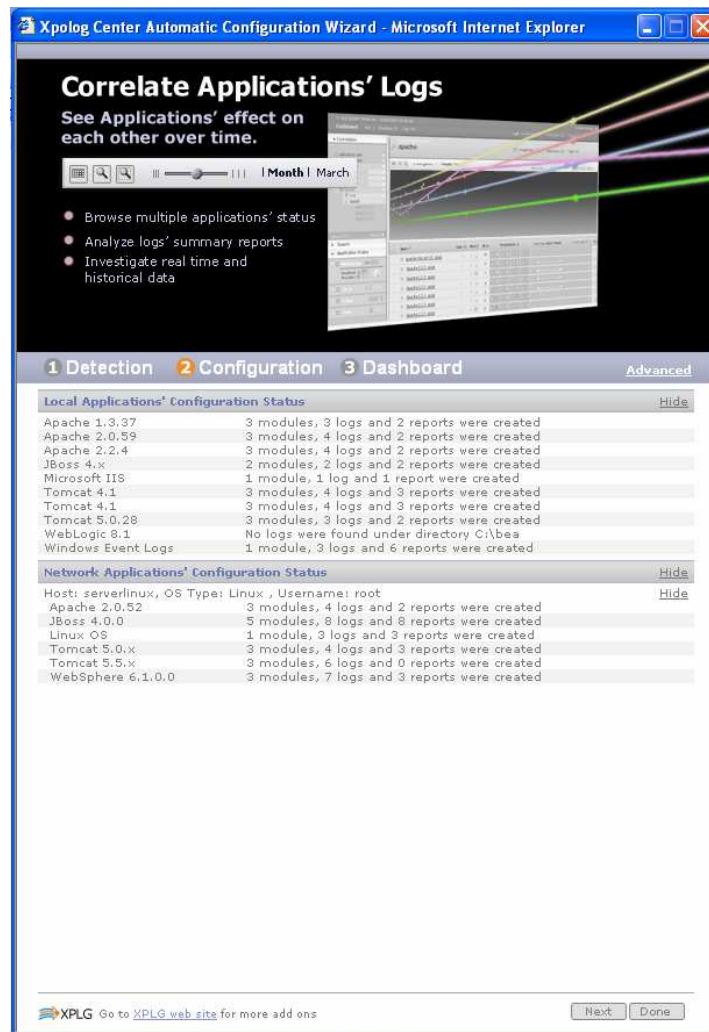
When finished adding all desired applications, click 'Next'



The automatic detection is now creating the configuration for all the selected applications.



When the configuration stage is finished, a list of all the modules, logs and reports created, both from local host and from the network is displayed.



At this point you can click 'Done', finish the automatic detection wizard and go back to XpoLog, or click 'Next', and the wizard will compute statistics and generate the reports created for the new logs added. The statistics computation and the report generation may be completed at a later time. For further information regarding statistics, please refer to Dashboard.



When the automatic detection process is done, you can either carry on configuring logs by clicking: ‘Configure more’ and you will be directed to the ‘data source administration’ in XpoLog’s main window.

Or, you may go to each one of the options listed on the right: Dashboard, Log Viewer, Search Engine, Reports, Diagnostics.

If you don’t want XpoLog to start the automatic configuration wizard every time XpoLog starts, mark the check box in the lower left corner of the detection wizard.

16. Create from Template:

The screenshot shows the XpoLog web interface. The top navigation bar includes 'XpoLog', 'XpoSearch', 'Dashboard', and a 'Home' link. Below this is a secondary navigation bar with 'Main', 'Administration', 'Configuration', 'Data Support', 'Reports', 'Settings', and 'Automation'. The left sidebar contains a 'Modules' section with a list of server types and a 'Verifiers' section with a dropdown menu. The main content area is titled 'Templates' and is divided into two sections: 'User defined templates' and 'System defined templates'. Each section contains a table with columns for 'Name', 'Description', and actions. The 'User defined templates' table lists 'XML' and 'Audit Log'. The 'System defined templates' table lists various log formats like '3ComFormat', 'ApacheAccess', 'Bluecoat', 'FireWall', 'IISLog', etc. Each row in the 'System defined templates' table has a 'create log' link. At the bottom of the page, there are 'previous' and 'cancel' links.

User defined templates		
Name	Description	
XML	http xml	create log delete
Audit Log		create log delete

System defined templates		
Name	Description	
3ComFormat		create log
ApacheAccess		create log
Bluecoat		create log
FireWall		create log
IISLog		create log
IIS Standard Log, please modify according to log header		create log
IsoTabUTCymd		create log
IsoTabymd		create log
KiwiCsvUtc		create log
KiwiCsvYmd		create log
KiwiTabdmy		create log
KiwiTabmdy		create log
KiwiUTCTabmdy		create log
KiwiUTCTab		create log
MailRelay		create log
Pix		create log
EqualProperties	Equal delimited properties file(key=value)	create log
Proxy		create log
Snort		create log
TabProperties	Tab delimited properties file(key value)	create log
WinFirewall		create log
WinMgmt		create log

A log can be created using predefined templates.

There are two kinds of templates: User defined and system defined.

For further information regarding the user defined templates please refer to configuration → Save as template.

Click the 'Create log' link opposite the desired log template you wish to add, and start configuring the log.

For example, adding the Apache access log using the Apache Access template.

The following log's wizard and the steps that needs to be done in order to finish this wizard, is similar to the 'Add log manually' paragraph, described in the administration→add log chapter.

17. Create from Wizard:

Name	Description	create log
Apache 1.x	Creates logs of Apache 1.x web server	create log
Apache 2.x	Creates logs of Apache 2.x web server	create log
Apache configuration	Create logs from apache configuration file.	create log
Java Logging Configuration	Create logs from java logging properties file.	create log
JBoss 4.x	Creates logs of JBoss 4.x application server	create log
Jetty server configuration	Create logs from jetty configuration file.	create log
Log4j	log4j wizard	create log
Microsoft IIS	Windows IIS Web Server	create log
Siebel	siebel wizard	create log
Siebel server configuration	Create logs from siebns.dat of siebel gateway	create log
Tomcat	tomcat wizard	create log
Tomcat 4.1.x	Creates logs of Tomcat 4.1.x application server	create log
Tomcat 5.0 configuration	Create logs from server.xml of tomcat	create log
Tomcat 5.0.x	Creates logs of Tomcat 5.0.x application server	create log
Tomcat 5.5 configuration	Create logs from tomcat logging.properties file.	create log
Tomcat 5.5.x	Creates logs of Tomcat 5.5.x application server	create log
WebLogic 10.0	Creates logs from WebLogic 10.0 domains	create log
WebLogic 8.1	Creates logs from WebLogic 8.1 domains	create log
WebLogic 9.2	Creates logs from WebLogic 9.2 domains	create log
WebLogic configuration	Create logs from webLogic configuration xml file.	create log
WebSphere	Creates logs of WebSphere application server	create log
WebSphere 6.x	Creates logs of WebSphere 6.x application server	create log
WebSphere configuration	Create logs from websphere configuration xml file.	create log
Windows Event Logs	Create windows event logs of network machines	create log

Creating a log using the system defined wizards helps you to add logs from a selected list of popular applications with minimum difficulty.

Select an application from the list, and click 'create log'.

For example, creating a log for Tomcat 4.1.x:

Click the 'create log' link, opposite 'Tomcat 4.1.x'

The screenshot shows the 'Wizard Admin' interface with the 'Location' step selected. The left sidebar contains a tree view of modules, including 'Examples', 'serverwin', 'qaserver', 'serverdb', 'Test', 'Apache 1.3.37', 'Apache 2.0.59', 'Apache 2.2.4', 'JBoss 4.x', 'IIS Web Server', 'Tomcat 4.1', 'Tomcat 4.1', 'Tomcat 5.0.28', 'Windows Event Logs', and 'Test for webserver'. The main content area has the following fields:

- Location**: Please specify the application's root full location path. Path:
- Select the account if connecting through SSH**: Account: [new](#)
- Please enter the IP or host name of the computer running the application**: Host:

At the bottom right, there are three buttons: [cancel](#), [previous](#), and [next](#).

Please specify the log's path, select an account if needed (If connecting thorough SSH) from the list of available accounts or create a new account, by clicking 'new' next to the accounts list. For further information regarding accounts, please refer to 'Data support → address book → SSH'. Specify the host name, or leave empty if the logs are located locally.

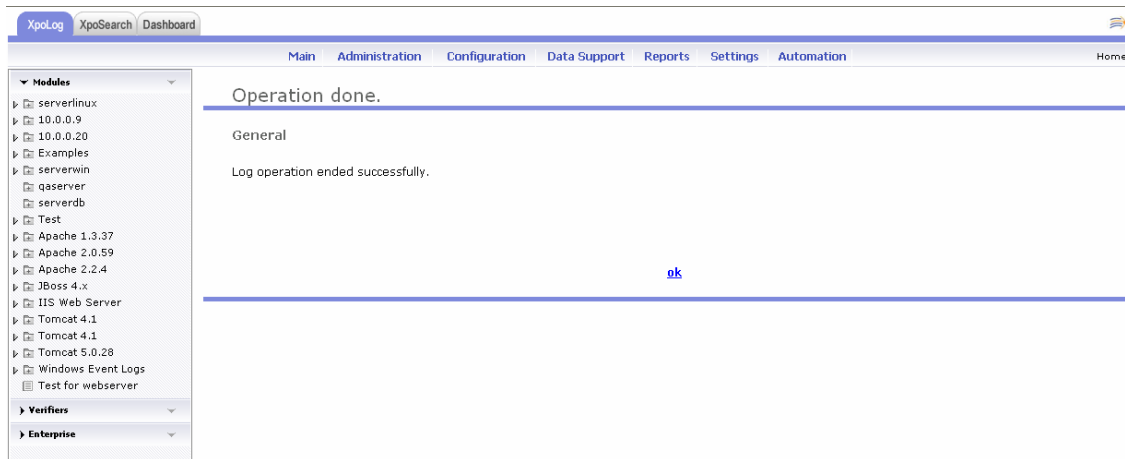
The screenshot shows the 'Wizard Admin' interface with the 'General' step selected. The left sidebar is the same as in the previous screenshot. The main content area has the following fields:

- General**: Parent module: New module name:
- Applications list**: Select applications to add and press next:
 - ☒ Tomcat 4.1.x
 - ☒ Configuration
 - ☒ server.xml
 - ☒ Logs
 - ☒ catalina_log
 - ☒ localhost_examples_log
 - ☒ localhost_log

At the bottom right, there are three buttons: [cancel](#), [previous](#), and [next](#).

Select a parent module for the log, or enter a new module name in the empty field (I.e. 'Tomcat 4.1' located inside module 'Configuration').

From the ‘Application list’, select all available logs for Tomcat 4.1.x. Click ‘Next’ and in the next screen, click ‘Ok’ to confirm the successful end of the wizard.



- **Edit log** - In order to edit an existing log via the administration menu, the specific log should be in focus. Select the relevant log in the left pane in the log viewer. When the log is in focus, open the administration menu and click 'Edit log'. The log's wizard (Similar to the add log wizard) is now available for you to make changes in it. Browse through the wizard using 'next' until completing it.
- **Edit log's permissions** – Editing the log's permissions enables you to set edit/view permissions for specific users/groups. Editing the log's permissions is only available when security is activated. For further information on security, please refer to Settings → General.

Select the relevant log in the left pane in the log viewer. When the log is in focus, open the administration menu and click 'Edit log's permissions'.

The screenshot shows the XpoLog administration interface. The top navigation bar includes 'Main', 'Administration', 'Configuration', 'Data Support', 'Reports', 'Settings', 'Security', 'Automation', 'Home', and 'Help'. The left sidebar shows a tree view of modules and verifiers. The main content area is titled 'Permissions' and contains two sections: 'Edit Group Members' and 'View Group Members'. Each section has 'Available Members' and 'Selected Members' lists with 'Add' and 'Remove' buttons. The 'Edit Group Members' section is currently active, showing 'Admin [user]', 'Administrators [group]', and 'All [group]' in the available list, and 'All [group]' in the selected list. The 'View Group Members' section is below it, with an empty selected list. At the bottom are 'Apply', 'Reset', and 'Cancel' buttons.

There are two options to set permissions:

1. 'Parent permissions' – this will set the same permissions as set in the parent module.
2. 'Use specified permissions' – selecting this option will allow you to add or remove users/groups from both available options: Edit group and the View group.

Click 'Reset' in case you would like to discard all changes, or click 'Apply' in order to save changes.

- **Edit log's Meta data** – Meta data selection – you can select a Meta data from a list of predefined Meta data schemes. For further information regarding Meta data, please refer to Data support → Meta data.

Properties – Application: select the most suitable application for the specific log from the list of predefined applications.

Specify the application version, build, platform, operating system and the vendor.

Add new property – you can add new property to the metadata by clicking ‘add new property’ link. New section will appear, enter the property type and value in the textboxes.

add new property

type	value	
<input type="text"/>	<input type="text"/>	remove

Add menu – you can add new search context by clicking ‘Add menu’ link. New section will appear, enter the search name in the ‘Name’ textbox and the search’s source in the path textbox.

Search Context Menu

Name	Path	
<input type="text"/>	<input type="text"/>	<div>Add Menu</div> <div>remove</div>

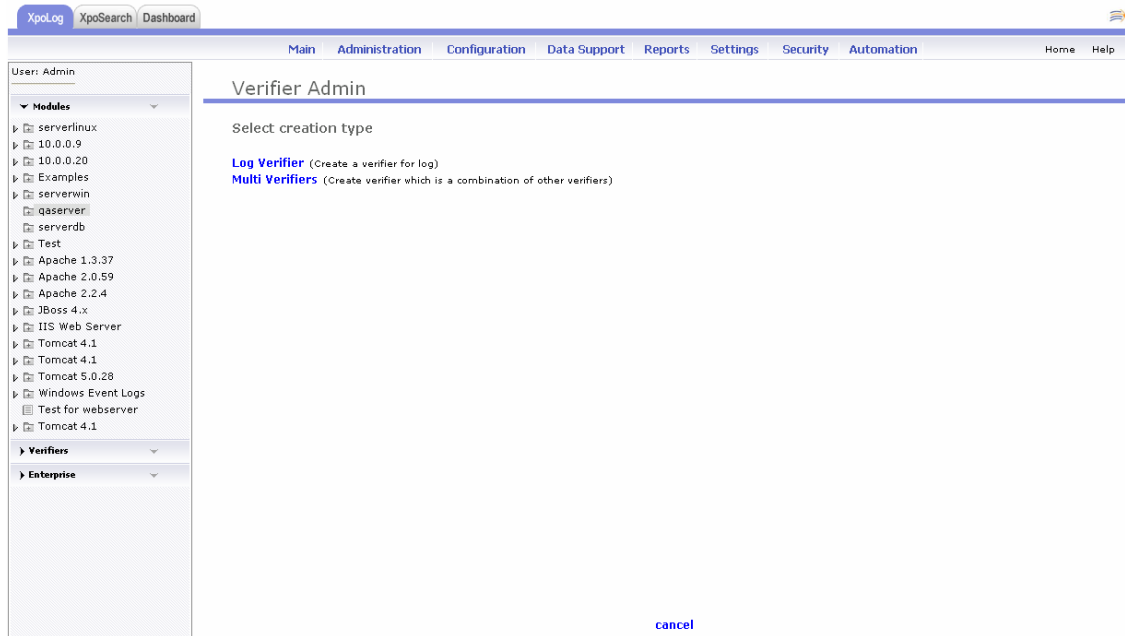
You can use the this metadata by right clicking on the relevant log view, selecting ‘Search’ and choosing the desire search context name.

The screenshot shows the XpoLog web interface. The top navigation bar includes tabs for XpoLog, XpoSearch, and Dashboard. Below this is a secondary navigation bar with links: Main, Administration, Configuration, Data Support, Reports, Settings, Security, Automation, Home, and Help. The left sidebar shows the user as 'Admin' and a tree view of modules and verifiers. The main content area is titled 'Meta data' and contains a 'Meta data selection' dropdown. Below this is a 'Properties' section with fields for Application, Version, Build, Platform, Operating system, and Vendor. The 'Platform' and 'Operating system' dropdowns are open, showing options like PC, Mac, AS/400, IBM RS6000, other, Windows, OS/2, Linux, OS X, and other. There is an 'add new property' link and a 'Search Context Menu' table at the bottom. The table has columns for Name and Path. At the bottom right is an 'Add Menu' link. At the bottom center are 'cancel' and 'save' buttons.

- Remove log** – in order to remove a log, select the relevant log in the left pane in the log viewer, and when the log is in focus, open the administration menu and click ‘Remove log’. Clicking ‘Ok’ will confirm deletion of log. In case you don’t want to delete it, click ‘Cancel’.

Verifier

Add verifier:



There are two different kinds of verifiers in XpoLog: Log verifier – works on a specific log, while Multi verifiers - is a combination of numerous log verifiers.

Log Verifier – A verifier is a mechanism that allows you to validate your system's health based on your logs and the filters defined for them. For instance, X number of 'ERROR' occurrences in the log may indicate that something is wrong. When you run a verifier (either manually or automatically) the verifier can execute different type of tasks according to the result. You can create multiple verifiers to examine the entire system state.

In the verifier’s wizard, specify a name for the verifier. Drill down in XpoLog’s tree to select the relevant log’s filter.

Check the ‘Scan log from last scan stop’ if you don’t want XpoLog to scan the whole log every time you activate the Verifier.

Rules – you can set failure/success rules for the verifier by specifying the number of results along with a relevant condition.

Actions – you may want XpoLog to execute a few actions in case the verifier fails/succeed. Use the add/remove commands in order to set a list of actions for

the verifier. For further information regarding tasks (Actions), please refer to Automation → Tasks.

Rules

Select the rules for this verifier:

Failure means that there are 10 records in the result.

Actions

execute following actions upon verifier **success**:

Actions

- Email - Error in log
- Execute task
- General Report task
- Report generation task
- URL Task

[add](#)
[add all](#)
[remove](#)
[remove all](#)

Execute actions

execute following actions upon verifier **failure**:

Actions

- Email - Error in log
- Execute task
- General Report task
- Report generation task
- URL Task

[add](#)
[add all](#)
[remove](#)
[remove all](#)

[show advanced options](#)

Advanced options – Failure – you can set XpoLog to execute a task upon verifier's failure only after X times it fails, instead of executing this task after each time the verifier fails.

Positive – you can set XpoLog to send a positive alert (A certain task) in 2 ways:

1. Set a time rule – Send a positive alert if the verifier doesn't fail in a certain time frame. I.e. – Send a positive alert 30 minutes after the last verifier's failure.
2. Send a positive alert after the next verifier's success. In that case, the time fields should be left empty.

The last thing you should configure is the task you would like XpoLog to execute as a positive alert.

[show advanced options](#)

Failure

Once failed, execute failure actions only after verifier failures

Positive

Execute positive alert(s) after from last failure

Note: if no positive alert settings are defined positive alert will be sent upon first verifier success following a verifier failure

execute following actions upon **positive alert** signal:

Actions

- Email - Error in log
- Execute task
- General Report task
- Report generation task
- URL Task

[add](#)
[add all](#)
[remove](#)
[remove all](#)

Execute actions

Click 'Save' to finish the verifier wizard.

Multi Verifier – multi verifiers is a selection of a few log verifiers all combined into one mechanism.

Specify a name for the multi verifier.

Settings – Add the desired verifiers to the ‘Selected’ list.

Rules – You may set a rule for the multi verifier, where at least one verifier or **all** verifiers fails, and execute a specific task accordingly.

Actions – add the actions XpoLog should execute in case of failure or success.

The screenshot shows the 'Multi Verifiers Settings' window in the XpoLog application. The interface includes a sidebar with a tree view of modules and verifiers. The main area is divided into sections for 'Global' settings, 'Settings' (including a list of available and selected verifiers), 'Rules' (for selecting rules and failure conditions), and 'Actions' (for configuring actions on success and failure). At the bottom, there are 'save', 'reset', and 'cancel' buttons.

User: Admin

Modules

- serverlinux
- 10.0.0.9
- 10.0.0.20
- Examples
- serverwin
- qserver
- serverdb
- Test
- Apache 1.3.37
- Apache 2.0.59
- Apache 2.2.4
- 2Boss 4.x
- IIS Web Server
- Tomcat 4.1
- Tomcat 5.0.28
- Windows Event Logs

Verifiers

- Verifier - Fatal
- Verifier - Debug
- Verifier - Warn
- Verifier - Error

Enterprise

Multi Verifiers Settings

Global

Name: [text box]

Settings

Select the verifiers to be used:

Available Verifiers

- Verifier - Debug
- Verifier - Error
- Verifier - Fatal
- Verifier - Warn

Add Remove

Selected Verifiers

Rules:

Select the rules for this verifier:

Failure means that: at least one verifier failed

Actions

execute following actions upon verifier success:

Actions

- Email - Error in log
- Execute task
- General Report task
- Report generation task
- URL Task

add add all remove remove all

Execute actions

execute following actions upon verifier failure:

Actions

- Email - Error in log
- Execute task
- General Report task
- Report generation task
- URL Task

add add all remove remove all

Execute actions

show advanced options

save reset cancel

Advanced options – Failure – you can set XpoLog to execute a task upon verifier’s failure only after X times it fails, instead of executing this task after each time the verifier fails.

Positive – you can set XpoLog to send a positive alert (A certain task) in 2 ways:

1. Set a time rule – Send a positive alert if the verifier doesn’t fail in a certain time frame. I.e. – Send a positive alert 30 minutes after the last verifier’s failure.
2. Send a positive alert after the next verifier’s success. In that case, the time fields should be left empty.

The last thing you should configure is the task you would like XpoLog to execute as a positive alert.

[show advanced options](#)

Failure
Once failed, execute failure actions only after verifier failures

Positive
Execute positive alert(s) after -select- from last failure
Note: if no positive alert settings are defined positive alert will be sent upon first verifier success following a verifier failure

execute following actions upon **positive alert** signal:

Actions		Execute actions
Email - Error in log	add add all remove remove all	
Execute task		
General Report task		
Report generation task		
URL Task		

Click 'Save' to finish the multi verifiers wizard.

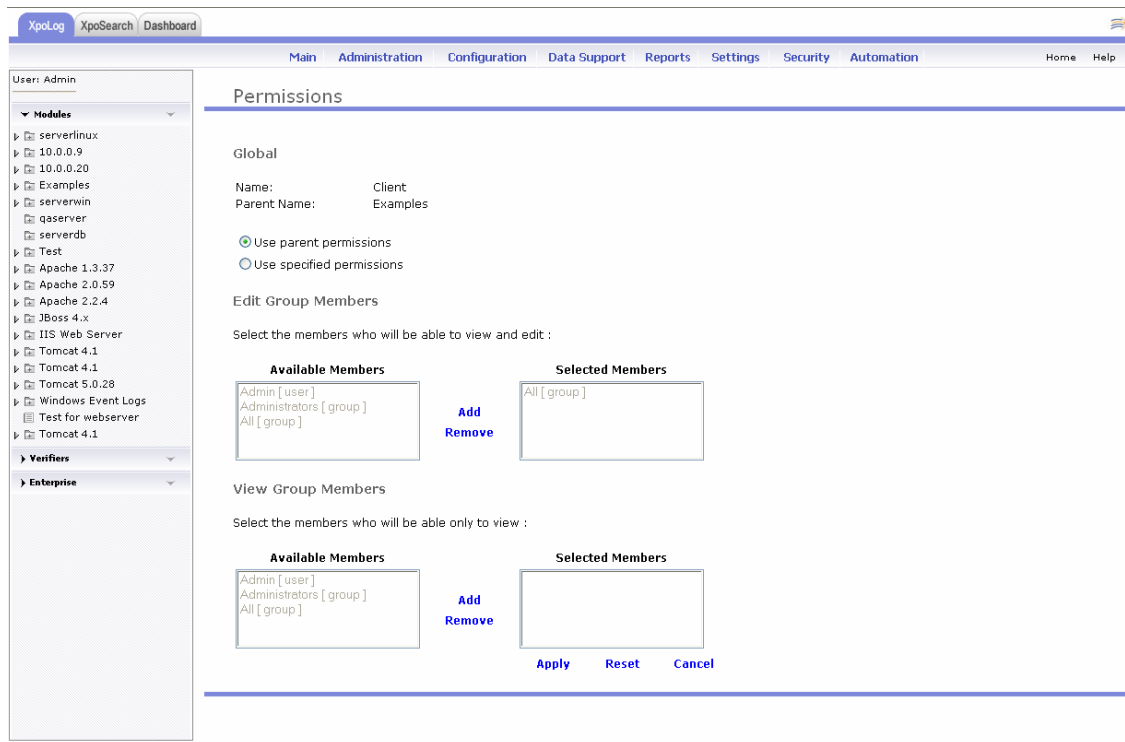
- **Edit verifier**

In order to edit an existing verifier via the administration menu, the specific verifier should be in focus. Select the relevant verifier in the left pane in the log viewer. When the verifier is in focus, open the administration menu and click 'Edit verifier'. The verifier's wizard (Similar to the add verifier wizard) is now available for you to make changes in it. When you are finished editing, click 'save'.

- **Edit verifier's permissions**

Editing the verifier's permissions enables you to set edit/view permissions for specific users/groups. Editing the verifier's permissions is only available when security is activated. For further information on security, please refer to Settings → General.

Select the relevant verifier in the left pane in the log viewer. When the verifier is in focus, open the administration menu and click 'Edit verifier's permissions'.



There are two options to set permissions:

1. 'Parent permissions' – this will set the same permissions as set in the parent module.
2. 'Use specified permissions' – selecting this option will allow you to add or remove users/groups from both available options: Edit group and the View group.

Click 'Reset' in case you would like to discard all changes, or click 'Apply' in order to save changes.

- **Edit verifier's Meta data**

Meta data selection – you can select a Meta data from a list of predefined Meta data schemes. For further information regarding Meta data, please refer to Data support → Meta data.

Properties – Application: select the most suitable application for the specific log from the list of predefined applications.

Specify the application version, build, platform, operating system and the vendor.

Add new property – you can add new property to the metadata by clicking ‘add new property’ link. New section will appear, enter the property type and value in the textboxes.



Add menu – you can add new search context by clicking ‘Add menu’ link. New section will appear, enter the search name in the ‘Name’ textbox and the search’s source in the path textbox.



You can use the this metadata by right clicking on the relevant log view, selecting ‘Search’ and choosing the desire search context name.

- **Remove verifier**

in order to remove a verifier, select the relevant verifier in the left pane in the log viewer, and when the verifier is in focus, open the administration menu and click ‘Remove verifier’. Clicking ‘Ok’ will confirm deletion of verifier. In case you don’t want to delete it, click ‘Cancel’.

Operation verification.

General

Are you sure you want to remove verifier - Verifier - Warn

cancel ok

Configuration Menu

Templates

Template is a complete configuration set for a certain file type, enables you to create logs in an easy way.

View Templates

For viewing templates select the 'Configuration' tab in the menu and then click 'View Templates'.

Templates		
User defined templates		
all a b c d e f g h i j k l m n o p q r s t u v w x y z		
Name	Description	
IIS access		create log delete
Appach httpd		create log delete
System defined templates		
all a b c d e f g h i j k l m n o p q r s t u v w x y z		
Name	Description	
3ComFormat		create log
ApacheAccess		create log
Bluecoat		create log
FireWall		create log
Froutier		create log
IISLog	IIS Standard Log, please modify according to log header	create log
IsoTabUTCymd		create log
IsoTabymd		create log
KiwCsvUtc		create log
KiwiCsvYmd		create log
KiwiTabdmy		create log
KiwiTabmdy		create log
KiwiUTCTabmdy		create log
KiwiUTCTab		create log
MailRelay		create log
Pix		create log
EqualProperties	Equal delimited properties file(key=value)	create log
Proxy		create log
Snort		create log
TabProperties	Tab delimited properties file(key value)	create log
WinFirewall		create log
WinMgmt		create log

The 'Template' page divided into two sections. 'System defined templates' and 'User defined templates'. 'System defined templates' are predefined configuration integrated with XpoLog software suite.

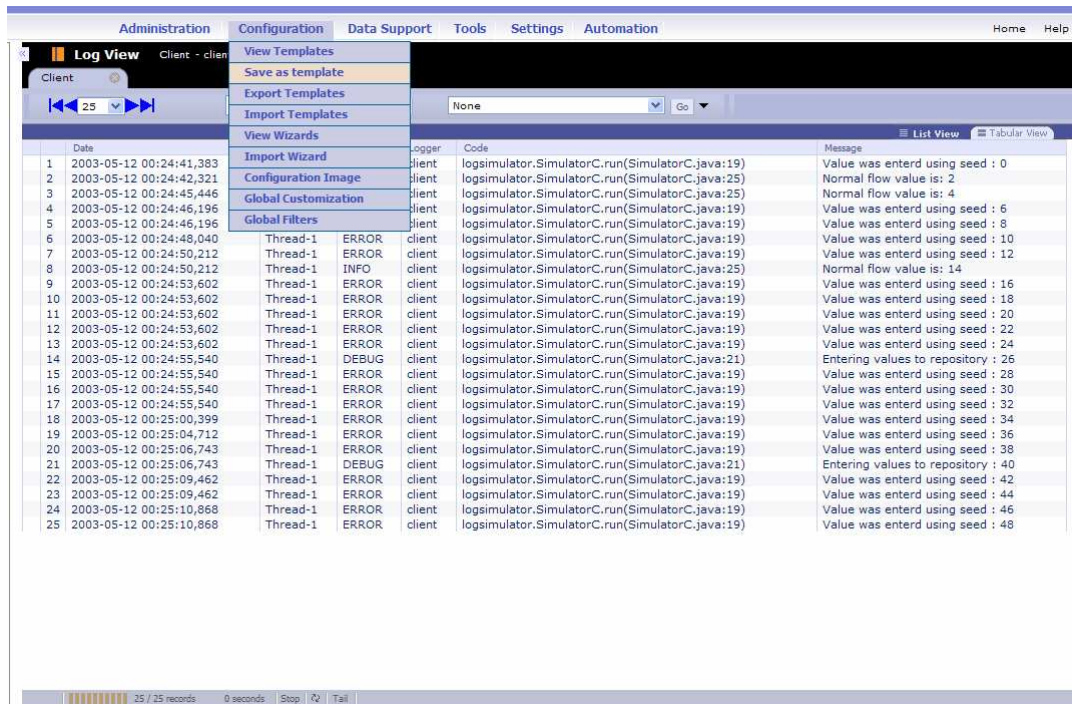
'User defined templates' are configurations sets created by the user.

In each section you can see all defined templates by clicking 'All' in the "ABC" bar or sort those defined templates by clicking the relevant letter.

In each section you can see the Template's name and description. For creating the log according to the selected template, click 'create log' link. This link will lead you to create

the log with all the log's definitions within the process (for farther information about creating logs see 'Add Log' section).

Saving a template



In order to save template, you have to select one log that his properties will be saved as the template. Then select 'Configuration' tab from the menu and click 'Save as template'.

Save template

General

Name

Client

Description

cancel

save

In the 'Name' textbox enter your template name. The default name is the log's name. Enter the description of the template in the 'Description' textbox (Optional). Click 'Save'.

Export Templates

Export Templates

Select the templates you want to export

	Name	Description
<input checked="" type="checkbox"/>	IIS access	
<input checked="" type="checkbox"/>	Appach httpd	

export

You can export your 'User defined templates' by selecting 'Configuration' and clicking 'Export Templates'. In this page, check the templates you want to export and click 'Export'. Save the zipped file in order to import it latter.

Import Templates

Import Templates

Location

Please specify XpoLog templates archive full location path or Network URL

Path

previous

next

You can import exported templates by selecting 'Configuration' and clicking 'Import Templates'. In this page, browse to the saved zipped file and click 'next'. The templates were added to your 'User defined templates'.

Wizards

XpoLog comes with a set of wizards that automate the process of adding configuration of modules, logs and reports of known applications to XpoLog.

View Wizards

For viewing the wizards select the 'Configuration' tab in the menu and then click 'View Wizards'.

Wizards		
System defined wizards		
Name	Description	
Apache 1.x	Creates logs of Apache 1.x web server	create log
Apache 2.x	Creates logs of Apache 2.x web server	create log
Apache configuration	Create logs from apache configuration file.	create log
Java Logging Configuration	Create logs from java logging properties file.	create log
JBoss 4.x	Creates logs of JBoss 4.x application server	create log
Jetty server configuration	Create logs from jetty configuration file.	create log
Microsoft IIS	Windows IIS Web Server	create log
SAP J2EE	SAP j2ee application wizard	create log
Siebel	siebel wizard	create log
Siebel server configuration	Create logs from siebns.dat of siebel gateway	create log
Tomcat 4.1.x	Creates logs of Tomcat 4.1.x application server	create log
Tomcat 5.0.x	Creates logs of Tomcat 5.0.x application server	create log
Tomcat 5.5 configuration	Create logs from tomcat logging.properties file.	create log
Tomcat 5.5.x	Creates logs of Tomcat 5.5.x application server	create log
WebLogic 10.0	Creates logs from WebLogic 10.0 domains	create log
WebLogic 8.1	Creates logs from WebLogic 8.1 domains	create log
WebLogic 9.2	Creates logs from WebLogic 9.2 domains	create log
WebLogic configuration	Create logs from webLogic configuration.xml file.	create log
WebSphere	Creates logs of WebSphere application server	create log
WebSphere 6.x	Creates logs of WebSphere 6.x application server	create log
WebSphere configuration	Create logs from websphere configuration.xml file.	create log
Windows Event Logs	Create windows event logs of network machines	create log
previous		cancel

In order to create the modules, logs and reports for the desired application, click 'create log' link.

The screenshot shows a web-based wizard interface titled "Wizard Admin". The current step is "Location". It contains three main sections: 1. A prompt "Please specify the application's root full location path" followed by a "Path" label and a text input field containing "C:\Program Files\Apache Software Foundation\Tomcat 5.5". 2. A prompt "Select the account if connecting through SSH" followed by an "Account" label and a dropdown menu showing "-- select --" with a "new" link next to it. 3. A prompt "Please enter the IP or host name of the computer running the application" followed by a "Host" label and an empty text input field. At the bottom of the form are three buttons: "cancel", "previous", and "next".

In the 'Path' textbox fill the application's root full location path. In case the wizard detected the application it will fill this textbox with the default application's path.

If you connected to the selected application through SSH connection or win authentication account, select the account from 'Account' select box or create new account. For further information regarding SSH and Windows authentication accounts, please refer to Data support → Address book.

If the selected application runs on remote machine, fill his IP or host name in the 'Host' textbox. Click 'next'.

Wizard Admin

General

Parent module

Modules

New module name:

Enter here the name of a new module to be created under the selected parent module
or leave this field empty to use only the selected parent module

Applications list

Select applications to add and press next:

☒ Tomcat 5.5.x

☒ Configuration

☒ server.xml

☒ Logs

☒ admin (Apache Tomcat log file)

☒ catalina (Apache Tomcat log file)

☒ host-manager (Apache Tomcat log file)

☒ localhost (Apache Tomcat log file)

☒ localhost_access_log

☒ manager (Apache Tomcat log file)

cancel

previous

next


In 'Wizard Admin' page, select the parent module for your selected modules and logs from 'Parent module' select box. By default to root module "Modules" is selected.

In 'New module name' enter the name of a new module to be created or leave this field empty to use only the selected parent module. Click 'next' to end this process.

95

Import Wizards

For import wizard select the 'Configuration' tab in the menu and then click 'Import Wizard'.



Import Wizard

Location

Please specify XpoLog wizard file full location path or Network URL

Path

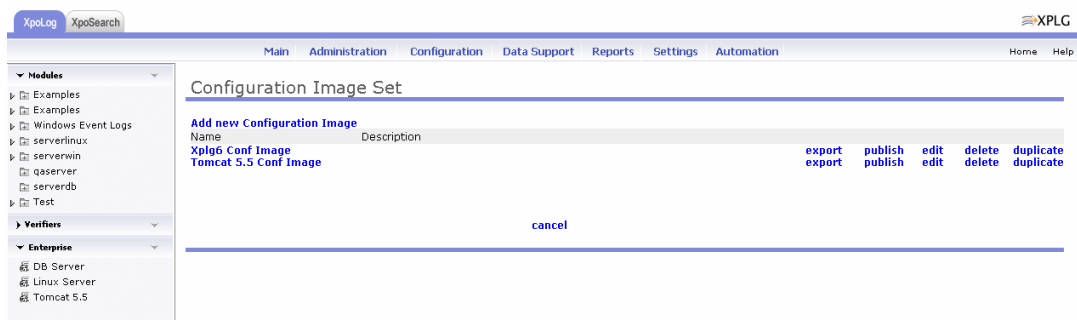
[previous](#) [next](#)

Browse to the wizard's zip file and click 'next'.

Configuration Image

A configuration image is the description of a set of XpoLog components, such as logs, reports, verifiers and so on. A configuration image can be exported and saved in the file system and could be later imported to created an identical configuration to the one that was saved.

From 'Configuration' menu select 'Configuration Image'



Add New Configuration Image:

To add new 'Configuration Image' click on 'Add new Configuration Image'.

The screenshot shows the 'Add New Configuration Image' form. It has a top navigation bar with 'Main', 'Administration', 'Configuration', 'Data Support', 'Reports', 'Settings', and 'Automation'. Below this is a tabbed interface with tabs: 'General', 'Meta Datas', 'Logs and modules', 'Verifiers', 'Accounts', 'Reports', 'Templates', and 'Wizards'. The 'General' tab is active, showing 'Configuration Image details'. There is a checkbox labeled 'Override existing configuration image'. Below it are text input fields for 'Name' and 'Description'. At the bottom are 'cancel' and 'save' buttons.

In the 'Name' text box enter your configuration image name. In the 'Description' text box enter its description (optional).

You can override existing configuration images by checking the 'Override existing configuration image' checkbox.

You can save your configuration image any time you want by clicking the 'save' link or 'Cancel' to go back to 'configuration Image' main page.

Adding Meta data configuration to your configuration image:

Select 'Meta Data' tab from menu and then select the desirable Meta data.

Configuration Image

General
Tasks

Meta Datas
Schedulers

Logs and modules
Enterprise

Verifiers

Accounts

Reports

Templates

Wizards

XpoLog Meta Data

Please check the meta datas you want to save in this configuration image.

☒ Tomcat 5.5.x (Tomcat 5.5.x application server logs)

☒ Windows Event Logs (Windows events)

☒ qa1 WebLogic 10.0 (WebLogic 10.0 application server logs)

☒ qa1 WebLogic 9.2 (WebLogic 9.2 application server logs)

☒ serverlinux Apache 2.0.52 (Apache 2.x web server logs)

☒ serverlinux JBoss 4.0.0 (JBoss 4.x application server logs)

☐ serverlinux Linux OS (Linux operating system logs)

☐ serverlinux Tomcat 5.0 (Tomcat 5.0.x application server logs)

☐ serverlinux Tomcat 5.5 (Tomcat 5.5.x application server logs)

☐ serverlinux WebSphere 6.1.0.0 (Creates logs of WebSphere 6.x application server)

☐ serverwin WebLogic 10.0 (WebLogic 10.0 application server logs)

☐ serverwin WebSphere 6.1.0.0 (Creates logs of WebSphere 6.x application server)

☐ serverwin Windows Event Logs (Windows events)

[select all](#) [clear all](#)

cancel

save

Adding logs and modules configurations to your configuration image:

Select 'Logs and Modules' tab from menu and then select the desirable logs and modules.

Configuration Image

General
Tasks

Meta Datas
Schedulers

Logs and modules
Enterprise

Verifiers

Accounts

Reports

Templates

Wizards

Available Modules and Logs

Please check the logs you want to save in this configuration image.

☒ Modules

☐ Examples

☒ Windows Event Logs

☒ Application

☐ Security

☒ System

☐ serverlinux

☐ serverwin

☐ qaserver

☒ serverdb

cancel

save

Adding verifiers' configurations to your configuration image:

Select 'Verifiers' tab from menu and then select the desirable verifiers and multi-verifiers.

Configuration Image

General **Meta Datas** **Logs and modules** **Verifiers** **Accounts** **Reports** **Templates** **Wizards**

Tasks **Schedulers** **Enterprise**

Verifiers hierarchy
Please check the verifiers you want to save in this configuration image.

☒ Verifiers

☒ ServerLinux

☒ Apach access

☐ Apach error

[cancel](#) [save](#)

Adding accounts configurations to your configuration image:

Select 'Accounts' tab from menu and then select the desirable accounts.

If you check the checkbox in the 'Override' column, the correlate accounts configuration will override the identical account configuration (if exist).

Configuration Image

General **Meta Datas** **Logs and modules** **Verifiers** **Accounts** **Reports** **Templates** **Wizards**

Tasks **Schedulers** **Enterprise**

XpoLog Accounts
Please check the accounts you want to save in this configuration image.

Name	Type	Description	Override
<input checked="" type="checkbox"/> MySQL User Xplg	db	user:xplg	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Oracle	db		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> PostgreSQL	db		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> SQL Server	db		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> auth xplg	winAuthentication		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> default: SQL DB	db		<input type="checkbox"/>
<input checked="" type="checkbox"/> ssh log	ssh		<input type="checkbox"/>
<input checked="" type="checkbox"/> ssh root@serverlinux	ssh		<input type="checkbox"/>
<input checked="" type="checkbox"/> ssh xplg@10.0.0.9	ssh		<input type="checkbox"/>
<input checked="" type="checkbox"/> xplg.com	http		<input type="checkbox"/>
<input checked="" type="checkbox"/> Check All			<input type="checkbox"/> Check All

[cancel](#) [save](#)

Adding reports configurations to your configuration image:

Select 'Reports' tab from menu and then select the desirable reports.

The screenshot shows a web application titled "Configuration Image". At the top, there is a horizontal menu with several tabs: "General Tasks", "Meta Datas Schedulers", "Logs and modules Enterprise", "Verifiers", "Accounts", "Reports", "Templates", and "Wizards". The "Reports" tab is currently selected and highlighted in blue. Below the menu, the main content area is titled "XpoLog Reports" and contains the instruction "Please check the reports you want to save in this configuration image." There is a list of eight reports, each with a checked checkbox: "access_log Status Aggregation", "Aggregation", "Client Date Aggregation", "LongFilterName", "WebLogic 9.2 > xplg > AdminServer > AdminServer > Severities", "wl_server > examplesServer > examplesServer > Message Ids", "xplg > AdminServer > access > Status + Remote Host (top 100)", and "xpologlog Text 5 Aggregation". Below the list, there are two links: "select all" and "clear all". At the bottom right of the form, there are two buttons: "cancel" and "save".

Adding templates configurations to your configuration image:

Select 'Templates' tab from menu and then select the desirable templates.

You can select 'User defined templates' that are templates that were created by the user and 'System templates' that are default templates added to the system.

Configuration Image

General Tasks	Meta Datas Schedulers	Logs and modules Enterprise	Verifiers	Accounts	Reports	Templates	Wizards
---------------	-----------------------	-----------------------------	-----------	----------	---------	-----------	---------

User defined templates

☒ Server

[select all](#) [clear all](#)

System templates

- ☒ 3ComFormat
- ☒ ApacheAccess
- ☒ Bluecoat
- ☒ FireWall
- ☒ Frouter
- ☒ IISLog - (IIS Standard Log, please modify according to log header)
- ☒ IsoTabUTCymd
- ☒ IsoTabymd
- ☒ KiwiCsvUtc
- ☒ KiwiCsvYMD
- ☒ MailRelay
- ☐ Pix
- ☐ EqualProperties - (Equal delimited properties file(key=value))
- ☐ Proxy
- ☐ Snort
- ☐ TabProperties - (Tab delimited properties file(key value))
- ☐ WinFirewall
- ☐ WinMgmt

[select all](#) [clear all](#)

[cancel](#) [save](#)

Adding wizards' configurations to your configuration image:

Select 'Wizards' tab from menu and then select the desirable wizards.

Configuration Image

General Tasks	Meta Datas Schedulers	Logs and modules Enterprise	Verifiers	Accounts	Reports	Templates	Wizards
---------------	-----------------------	-----------------------------	-----------	----------	---------	-----------	---------

XpoLog Wizards

Please check the wizards you want to save in this configuration image.

- ☒ Apache 1.x - (Creates logs of Apache 1.x web server)
- ☒ Apache 2.x - (Creates logs of Apache 2.x web server)
- ☒ Apache configuration - (Create logs from apache configuration file.)
- ☒ Java Logging Configuration - (Create logs from java logging properties file.)
- ☒ JBoss 4.x - (Creates logs of JBoss 4.x application server)
- ☒ Jetty server configuration - (Create logs from jetty configuration file.)
- ☒ Microsoft IIS - (Windows IIS Web Server)
- ☒ SAP J2EE - (SAP j2ee application wizard)
- ☒ Siebel - (siebel wizard)
- ☒ Siebel server configuration - (Create logs from siebns.dat of siebel gateway)
- ☒ Tomcat 4.1.x - (Creates logs of Tomcat 4.1.x application server)
- ☒ Tomcat 5.0.x - (Creates logs of Tomcat 5.0.x application server)
- ☒ Tomcat 5.5 configuration - (Create logs from tomcat logging.properties file.)
- ☒ Tomcat 5.5.x - (Creates logs of Tomcat 5.5.x application server)
- ☒ WebLogic 10.0 - (Creates logs from WebLogic 10.0 domains)
- ☒ WebLogic 8.1 - (Creates logs from WebLogic 8.1 domains)
- ☒ WebLogic 9.2 - (Creates logs from WebLogic 9.2 domains)
- ☒ WebLogic configuration - (Create logs from webLogic configuration.xml file.)
- ☒ WebSphere - (Creates logs of WebSphere application server)
- ☒ WebSphere 6.X - (Creates logs of WebSphere 6.x application server)
- ☒ WebSphere configuration - (Create logs from websphere configuration.xml file.)
- ☒ Windows Event Logs - (Create windows event logs of network machines)

[select all](#) [clear all](#)

[cancel](#) [save](#)

Adding tasks configurations to your configuration image:

Select 'Tasks' tab from menu and then select the desirable tasks.

If you check the checkbox in the 'Override' column, the correlate task configuration will override the identical task configuration (if exist).

The screenshot shows the 'Configuration Image' interface for 'XpoLog Tasks'. At the top, there is a navigation bar with tabs: General Tasks, Meta Datas Schedulers, Logs and modules Enterprise, Verifiers, Accounts, Reports, Templates, and Wizards. The 'General Tasks' tab is selected. Below the navigation bar, the title 'XpoLog Tasks' is displayed, followed by the instruction 'Please check the tasks you want to save in this configuration image.' A table with four columns: Name, Type, Description, and Override, lists the tasks. The tasks are: Email alert (Type: email, Override: checked), Jms task (Type: JmsTask, Override: checked), and web logic report (Type: reports, Override: checked). At the bottom of the table, there is a 'Check All' row with a checked checkbox in the Name column and a checked checkbox in the Override column. Below the table, there are 'cancel' and 'save' buttons.

Name	Type	Description	Override
<input checked="" type="checkbox"/> Email alert	email		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Jms task	JmsTask		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> web logic report	reports		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Check All			<input checked="" type="checkbox"/> Check All

cancel save

Adding schedulers' configurations to your configuration image:

Select 'Schedulers' tab from menu and then select the desirable schedulers.

If you check the checkbox in the 'Override' column, the correlate scheduler configuration will override the identical scheduler configuration (if exist).

The screenshot shows the 'Configuration Image' interface for 'XpoLog Schedulers'. At the top, there is a navigation bar with tabs: General Tasks, Meta Datas Schedulers, Logs and modules Enterprise, Verifiers, Accounts, Reports, Templates, and Wizards. The 'Meta Datas Schedulers' tab is selected. Below the navigation bar, the title 'XpoLog Schedulers' is displayed, followed by the instruction 'Please check the schedulers you want to save in this configuration image.' A table with four columns: Name, Type, Description, and Override, lists the schedulers. The schedulers are: Email alert (Type: op, Override: unchecked), Verifier Apach access log (Type: verifier, Override: unchecked), and WebLogic reports (Type: op, Override: unchecked). At the bottom of the table, there is a 'Check All' row with a checked checkbox in the Name column and an unchecked checkbox in the Override column. Below the table, there are 'cancel' and 'save' buttons.

Name	Type	Description	Override
<input checked="" type="checkbox"/> Email alert	op		<input type="checkbox"/>
<input checked="" type="checkbox"/> Verifier Apach access log	verifier		<input type="checkbox"/>
<input checked="" type="checkbox"/> WebLogic reports	op		<input type="checkbox"/>
<input checked="" type="checkbox"/> Check All			<input type="checkbox"/> Check All

cancel save

Adding enterprises configurations to your configuration image:

Select 'Enterprises' tab from menu and then select the desirable enterprises.

Configuration Image

General Tasks Meta Datas Schedulers **Logs and modules Enterprise** Verifiers Accounts Reports Templates Wizards

XpoLog Nodes

Please check the nodes you want to save in this configuration image.

Name	Description	Override
<input checked="" type="checkbox"/> DB Server		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Linux Server		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Tomcat 5.5		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Check All		<input checked="" type="checkbox"/> Check All

[cancel](#) [save](#)

If you already have a configuration image you can edit, duplicate or delete it by clicking the matching links.

Publish existing Configuration Image

The publish action allows you to publish an existing configuration image to other XpoLog node or to your local XpoLog node.

Do that by clicking on the 'Publish' link.

Publishers Set

[Add new Publisher](#)

Name	
<input type="checkbox"/> Default	edit delete duplicate

[previous](#) [publish](#) [save](#) [cancel](#)

If you want to use the default publisher, check the 'Default' checkbox. You can also edit, delete or duplicate this publisher by clicking the matching link.

In order to create new publisher click the 'Add new Publisher' link.

Configuration Image module names

Module names

Name:

Please specify for each module the name it will have in the target machine.

Local module name	New module name
Windows Event Logs	<input type="text" value="Windows Event Logs"/>
serverwin	<input type="text" value="serverwin"/>
WebSphere 6.1.0.0	<input type="text" value="WebSphere 6.1.0.0"/>
AppSrv01	<input type="text" value="AppSrv01"/>
SERVERWINNode01	<input type="text" value="SERVERWINNode01"/>
server1	<input type="text" value="server1"/>
AppSrv02	<input type="text" value="AppSrv02"/>
SERVERWINNode02	<input type="text" value="SERVERWINNode02"/>
server1	<input type="text" value="server1"/>
Modules	<input type="text" value="Modules"/>

[previous](#) [next](#) [cancel](#)

In the 'Name' textbox enter the publisher's name. For each (local) module you can give new name that will be assigned while importing. Click 'Next'.

Configuration Image logs paths

Log paths

Please specify for each log the destination path that it will have in the target machine.

Global	Local path	Target path
1.	<input type="text"/>	<input type="text"/>
Log Name	Local path	Target path
SystemErr	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
SystemErr	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
SystemOut	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
SystemOut	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
http_access	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
http_access	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
http_error	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
http_error	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
native_stderr	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
native_stderr	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
native_stdout	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
native_stdout	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
trace	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>
trace	<input type="text" value="\\serverwin\c\$\Program Files\IBM\WebSphere\AppServer\"/>	<input type="text" value="update identical"/>

leave target path blank to use local path

[previous](#) [next](#) [cancel](#)

In The logs paths page you can change the target logs paths. In the 'Global' section you can give a local global path, that all the local logs located in that path, will get new path at the target machine. Enter the new target path in the 'Target path' textbox.

You can do the same action for each log separately at the 'Log Name' section. Click 'Next'.

Publish to nodes

XpoLog Enterprise Nodes

Select the XpoLog Enterprise Nodes you want to publish the configuration image to

☒ local Xpolog Node

[select all](#) [clear all](#)

☒ 10.0.3.10
☐ 10.0.3.44
☒ Server Linux
☐ Server Windows

[previous](#) [next](#)

In 'Publish to nodes' page you decide to which nodes you want to publish the configuration image. Check the 'local XpoLog Node' checkbox if you want to publish this image to your local machine. Check any other enterprise nodes (if exist) for remote publishing. Click 'Next'.

Publishers Set

[Add new Publisher](#)

Name			
<input type="checkbox"/> Default	edit	delete	duplicate
<input checked="" type="checkbox"/> My Publisher	edit	delete	duplicate

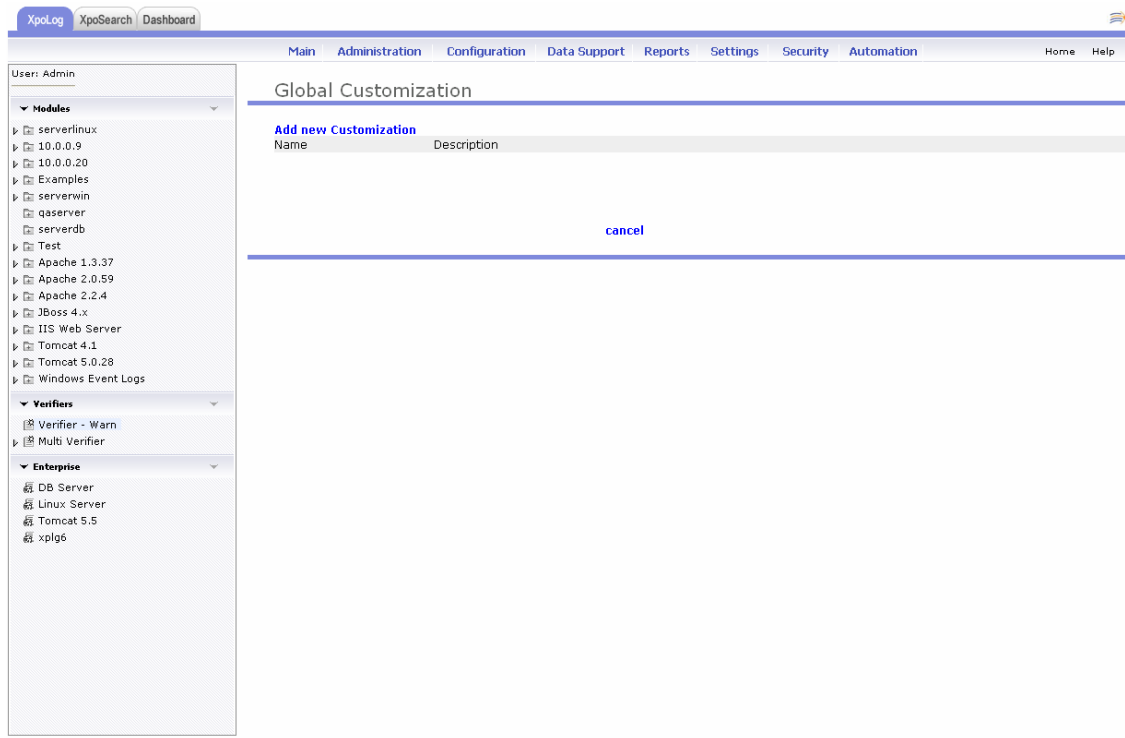
[previous](#) [publish](#) [save](#) [cancel](#)

Select the publisher you want to use by checking its checkbox and then click 'Save' to save the publisher definition or click 'Publish' for publishing the configuration image by the selected publisher.

Global Customization

Add new customization - Global customization allows you to change a few general logs settings, such as table customizing, color selection and log view options.

To add a new global customization, from the configuration menu select ‘Global customization’



Click ‘Add new customization’ in order to start the wizard.

XpoLog
XpoSearch
Dashboard

Main
Administration
Configuration
Data Support
Reports
Settings
Security
Automation
Home
Help

User: Admin

Modules
serverlinux
10.0.0.9
10.0.0.20
Examples
serverwin
qaserver
serverdb
Test
Apache 1.3.37
Apache 2.0.59
Apache 2.2.4
JBoss 4.x
IIS Web Server
Tomcat 4.1
Tomcat 5.0.28
Windows Event Logs

Verifiers
Verifier - Warn
Multi Verifier

Enterprise
DB Server
Linux Server
Tomcat 5.5
xplg6

Global Customization

Selected Log
access
Name
new customization
Description

Type
Date
Source
Category
Event
User
Computer
Description

add
remove

Type
Date
Source
Category
Event
User
Computer
Description

Move up
Move down

Priority color selection

Error paint in
Warning paint in
Information paint in
Success paint in
Failure Audit paint in
Success Audit paint in

0020DF
4080BF
008040
209F00
9F4000
80009F

pick color
pick color
pick color
pick color
pick color
pick color

Log Search Settings
☒ When checked - a search and filter result will be presented from the beginning of the log
(Note: when unchecked the result is on current view)

Log Start Operation
When viewing a log that compound of several files, you may choose from which file to start your view.

☒ View from the beginning of the most updated file
☐ View from the beginning of the oldest file
☐ View from the end of the most updated file

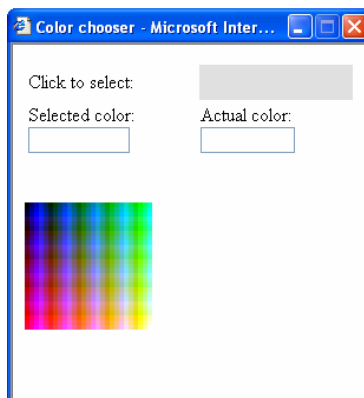
cancel
save

First of all, select the log you wish to customize from the list of the available logs in XpoLog.

Specify a name and description for the customization.

Table customization – you may add or remove columns from the log, and you can set their order by moving them up/down.

Priority color selection – you can select the color of each one of the priorities in the list, by clicking the ‘Pick color’ link, and choosing the desired color.



Log search settings - check this option in case you would like XpoLog to present a search and filter result from the beginning of the log

Log start operation - In case a log is compound of more then one file, you may select the file display order as following:

View from the beginning of the most updated file

View from the beginning of the oldest file

View from the end of the most updated file

Click 'save' when done configuring the log's customization, or 'cancel' to discard changes.

Edit global customization

The global customizations can be edited in the future. Click 'Global customization' in the configuration menu, and click 'edit' next to the customization you wish to edit.

Global Customization		
Add new Customization		
Name	Description	
Access log		edit delete
Apache log		edit delete
Application log		edit delete
Tomcat log		edit delete
cancel		

Delete global customization

In case you would like to remove a global customization, click the 'delete' link opposite to the relevant customization name.

Global Filters

A global filter enables you to create a single filter that will be available for all logs using the same log pattern. This feature saves you the time of creating dozens of regular filters for every log, when all these logs are using the same pattern.

The screenshot shows the XpoLog web interface. The top navigation bar includes tabs for XpoLog, XpoSearch, and Dashboard. Below this is a menu bar with links: Main, Administration, Configuration, Data Support, Reports, Settings, Security, Automation, Home, and Help. On the left, a sidebar shows the user as 'Admin' and a tree view of modules and verifiers. The main content area is titled 'Global Filters' and contains links for 'Add new Filter' and 'Add new Multi Filter'. Below these links is a table with columns 'Name', 'Description', and 'Type'. A 'cancel' button is visible at the bottom of the table area.

There are 2 different kinds of global filters: **Global filters** and **Multi filters**.

Add new global filter – Select the log you wish to create a global filter to from the list of XpoLog's logs. The whole wizard will refresh according to the selected log. You may select one of the log's predefined filters, and the wizard will update itself according to the specific filter's properties.

The screenshot shows the 'Global Filter definition' page in XpoLog. The left sidebar is identical to the previous screenshot. The main content area is titled 'Global Filter definition' and contains several sections for configuring the filter. The 'Selected Log' is set to 'access' and the 'Selected Filter' is '-new filter-'. The 'Name' field is 'GenFilterName_1' and the 'Description' field is empty. The 'Date and Time' section has a radio button selected for 'Dates limit'. Below this are two options: 'Show records that arrive after' and 'Show records that arrive before', both with date pickers and a 'calendar' button. The 'show records from the' section has a radio button selected for 'last' and a dropdown for 'hours'. The 'Number' section has a 'Column: Status' dropdown set to 'equals' and an empty input field. The 'Text' section has four rows, each with a 'Show records that' label, a dropdown set to 'contain', a 'the text' label, an empty input field, a 'case sensitive' checkbox, and a 'regular expression' checkbox. At the bottom, there are 'save', 'cancel', and 'help' buttons.

In case you would like to create a new filter, please specify a name and description to the new filter.

Date and time – you may set date limits for the filter, using the ‘dates limit’ fields, or leave it blank and not limit the filter at all.

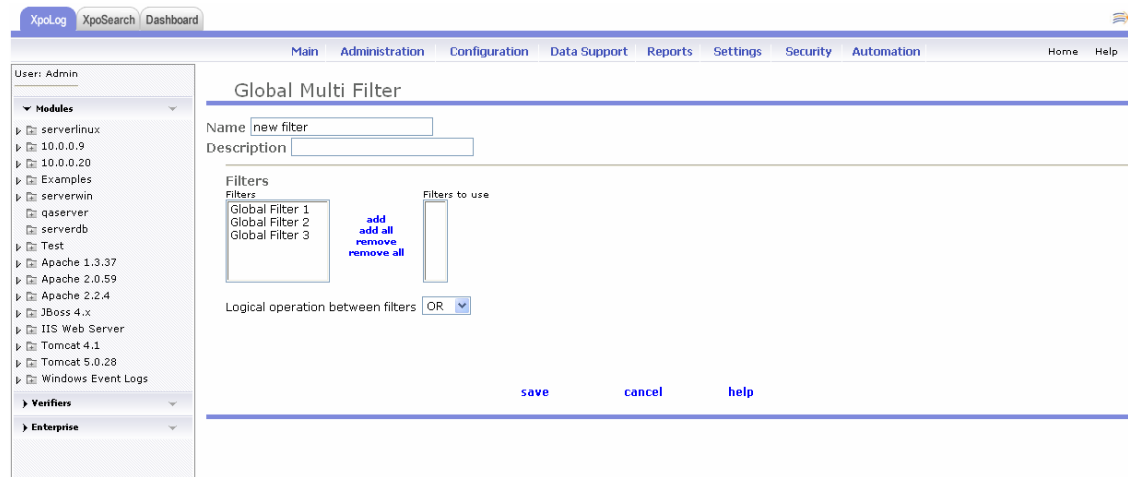
Number/Text – in these fields you should add the relevant information you would like to filter from the specific log.

When you finished configuring the global filter, click ‘Save’ or click ‘Cancel’ to discard changes.

Add new multi global filter

The multi filter is combination of a few global filters.

Click the ‘add new multi filter’



The screenshot shows the 'Global Multi Filter' configuration page in the XpoLog application. The interface includes a top navigation bar with tabs for XpoLog, XpoSearch, and Dashboard. Below this is a main navigation menu with options like Main, Administration, Configuration, Data Support, Reports, Settings, Security, Automation, Home, and Help. On the left, a sidebar shows a tree view of modules and verifiers. The main content area is titled 'Global Multi Filter' and contains fields for 'Name' (set to 'new filter') and 'Description'. Below these fields, there are two columns: 'Filters' and 'Filters to use'. The 'Filters' column lists 'Global Filter 1', 'Global Filter 2', and 'Global Filter 3'. Between these columns are buttons for 'add', 'add all', 'remove', and 'remove all'. Below the columns, there is a dropdown for 'Logical operation between filters' set to 'OR'. At the bottom right, there are 'save', 'cancel', and 'help' buttons.

Specify a name and description for the new multi filter.

From the list of available filters add at least two filters, and specify the logical operation (or/and) between those filters.

Edit global filter/Multi filter

The global filter/multi filter can be edited at any time. Click ‘Global filter’ in the configuration menu, and click ‘edit’ next to the filter/multi filter you wish to edit.

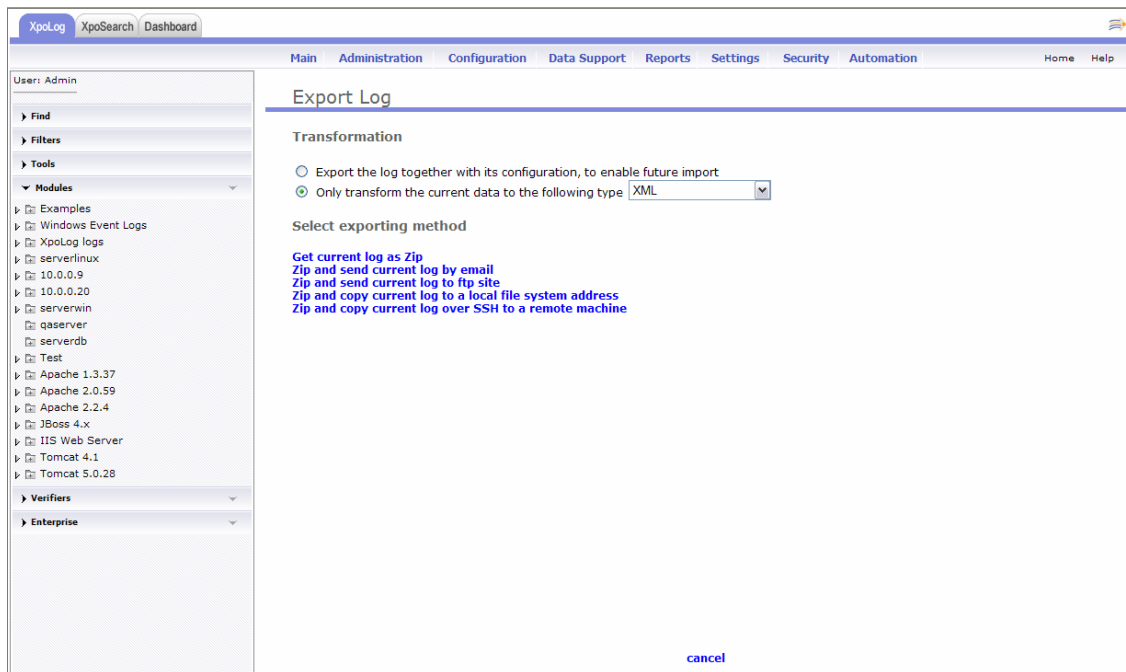
Click ‘save’ when done or ‘cancel’ to discard changes.

Delete global customization

In case you would like to remove a global filter/multi filter, click the ‘delete’ link opposite to the relevant filter/multi filter’s name.

Data Support Menu

Export Log



All logs can be exported from XpoLog in one of the two following ways:

1. The log is exported with its configuration, in case you would like to import it again in the future.
2. Only the log's data is exported. The log's configuration will be lost. There are 4 different types you can transform the current data to: XML, CSV, Tab Delimited, and SQL DB table.

Export Log

Transformation

☐ Export the log together with its configuration, to enable future import
 ☒ Only transform the current data to the following type

Select exporting method

Get current log as Zip
 Zip and send current log by email
 Zip and send current log to ftp site
 Zip and copy current log to a local file system address
 Zip and copy current log over SSH to a remote machine

XML
 CSV
 TAB Delimited
 SQL Database Table

In order to export a log, select the relevant log in the left pane in the log viewer, and when the log is in focus, open the data support menu, and select the export log option. Choose the desired transformation type (With or without the log's configuration), and click the desired exporting method, from the following available options:

Get current log as zip

Selecting this option will save the current log as a zip file. You can open the zip file or save it for future use.

Export Log

Transformation

☐ Export the log together with its configuration, to enable future import
 ☒ Only transform the current data to the following type

Select exporting method

Get current log as Zip
 Zip and send current log by email
 Zip and send current log to ftp site
 Zip and copy current log to a local file system address
 Zip and copy current log over SSH to a remote machine

XML
 CSV
 TAB Delimited
 SQL Database Table

Zip and send current log by email

The log will be sent via email, as a zip file.

Select an email account for both the sender and the receiver of this email, from the list of the predefined email accounts, or create a new email account by clicking ‘new’. For further information regarding email accounts, please refer to Data support → Address book.

Add a subject for this email, and add text if required. Click ‘next’ in order to send the email.

Zip and send current log to an FTP site

The log will be sent to an FTP site.

In the FTP address, select an FTP account, or click ‘new’ in order to configure a new one. For further information regarding FTP accounts, please refer to Data support → Address book.

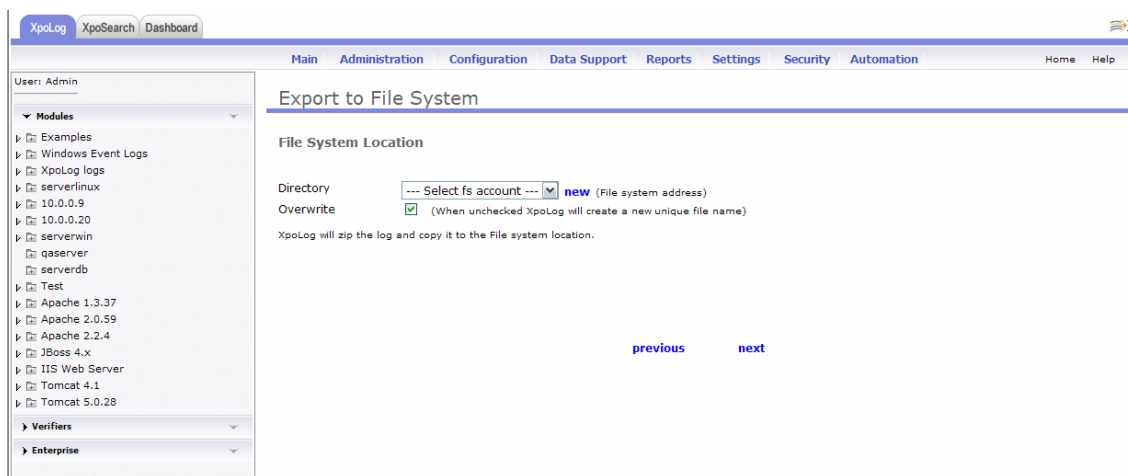
Specify the FTP site directory, in which the log will be saved, and click ‘next’ to start the transfer process.

Zip and copy current log to a local FS address

The log will be copied to a local file system address on your machine. From the 'Directory' combo box select the FS account you wish to save the log to, or click 'new' in order to configure a new FS account. For further information regarding FS accounts, please refer to Data support → Address book.

Check the 'Overwrite' option in case you would like XpoLog to overwrite an existing similar file.

Click 'next' to start the transfer process.



Zip and copy current log over SSH to a remote machine

The log will be transferred over SSH to a remote machine. Select an SSH account from the list of available SSH accounts, or click new in order to configure a new SSH account. For further information regarding SSH accounts, please refer to Data Support → Address book.

Specify the directory on the remote machine, in which XpoLog will copy the log to.

Click 'next' to start the transfer over SSH process.

XpoLogXpoSearchDashboard

MainAdministrationConfigurationData SupportReportsSettingsSecurityAutomationHomeHelp

User: Admin

Modules

Examples

Windows Event Logs

XpoLog logs

serverlinux

10.0.0.9

10.0.0.20

serverwin

qaserver

serverdb

Test

Apache 1.3.37

Apache 2.0.59

Apache 2.2.4

JBoss 4.x

IIS Web Server

Tomcat 4.1

Tomcat 5.0.28

Verifiers

Enterprise

Export via SSH

SSH details

SSH Address

--- Select ssh account ---new

Directory/

XpoLog will zip the log and copy it to the specified location.

previous

next

Import Log

You can import to XpoLog any kind of log, as long as it was exported with its configuration.

Specify the log's path, and click 'Next'.

Import log

Location

Please specify XpoLog archive file full location path

Path

Browse...

Note: It is only possible to import archives that were created with XpoLog version 2.2 and above.

[previous](#) [next](#)

After finding the desired log, please select a parent module from the list of available modules.

Import log

Import module

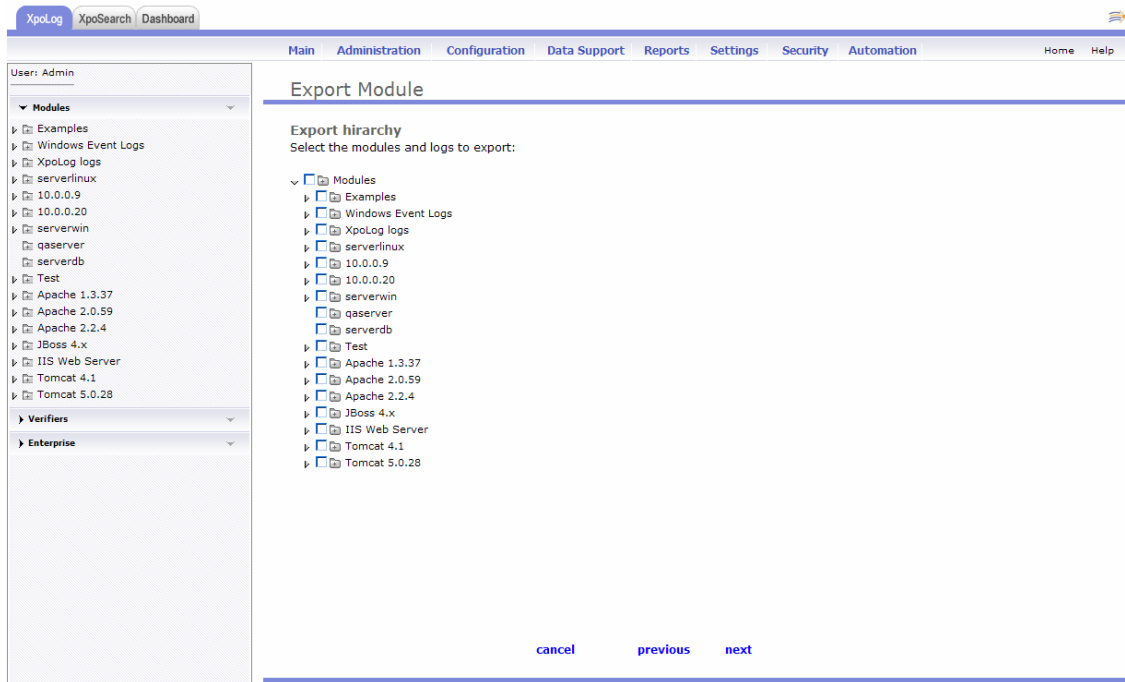
Import wizard found log **SNMP Test** in the archive. Please select parent module for the log and press next.

Parent module

[cancel](#) [previous](#) [next](#)

Click 'next' to finish the import process or 'previous' in case you would like to import a different log. Click 'Ok' to confirm the successful import.

Export Module



In order to export a module from XpoLog, make your selection in XpoLog module's tree, and click 'Next'. There are five different export methods to choose from:

Select exporting media
[Zip and download](#)
[Zip and send by email](#)
[Zip and send by ftp site](#)
[Zip and copy to a local file system address](#)
[Zip and copy to remote machine via SSH](#)

Zip and download

Selecting this option will save the current module as a zip file. You can open the zip file or save it for future use.

Zip and send by email

The module will be sent via email, as a zip file.

Select an email account for both the sender and the receiver of this email, from the list of the predefined email accounts, or create a new email account by clicking ‘new’. For further information regarding email accounts, please refer to Data support → Address book.

Add a subject for this email, and add text if required. Click ‘next’ in order to send the email.

Zip and send to an FTP site

The module will be sent to an FTP site.

In the FTP address, select an FTP account, or click ‘new’ in order to configure a new one. For further information regarding FTP accounts, please refer to Data support → Address book.

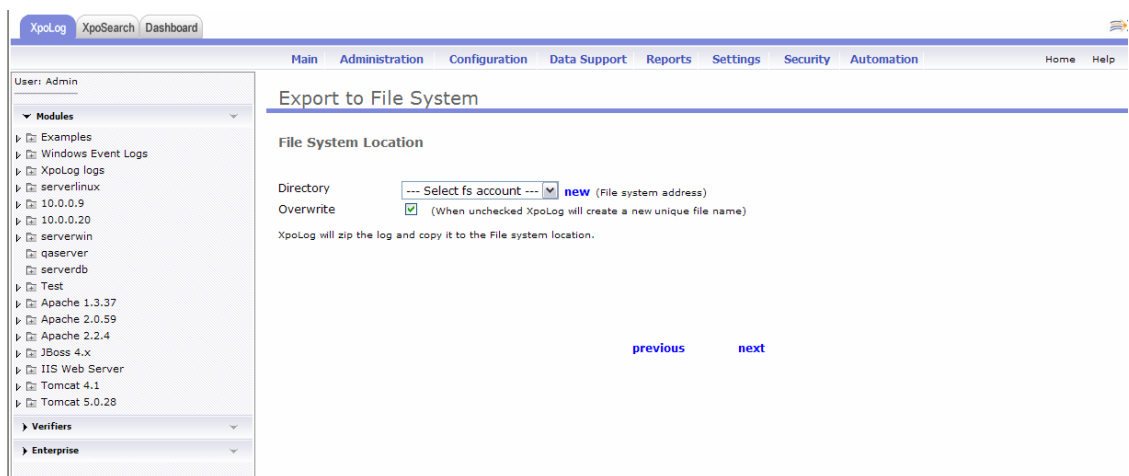
Specify the FTP site directory, in which the module will be saved, and click ‘next’ to start the transfer process.

Zip and copy to a local FS address

The module will be copied to a local file system address on your machine. From the 'Directory' combo box select the FS account you wish to save the module to, or click 'new' in order to configure a new FS account. For further information regarding FS accounts, please refer to Data support → Address book.

Check the 'Overwrite' option in case you would like XpoLog to overwrite an existing similar file.

Click 'next' to start the transfer process.

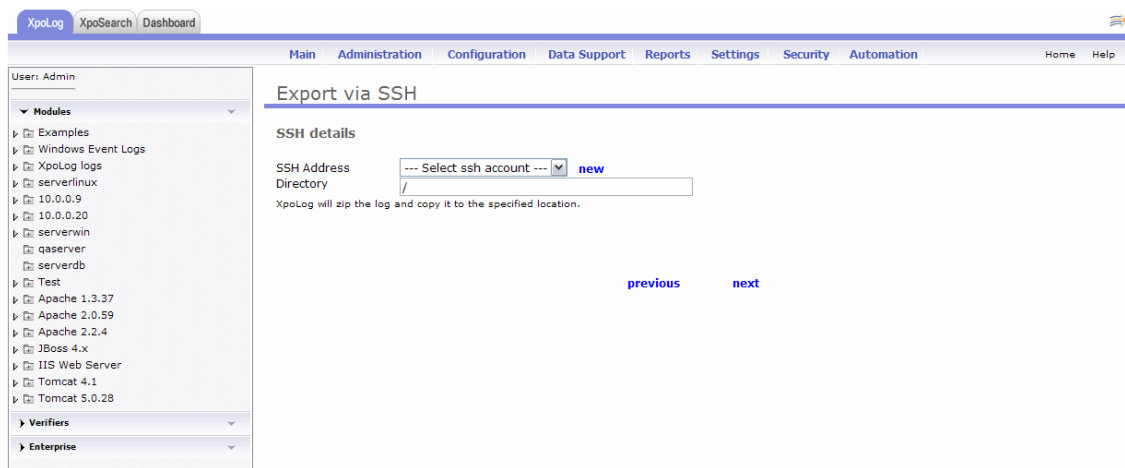


Zip and copy to remote machine over SSH

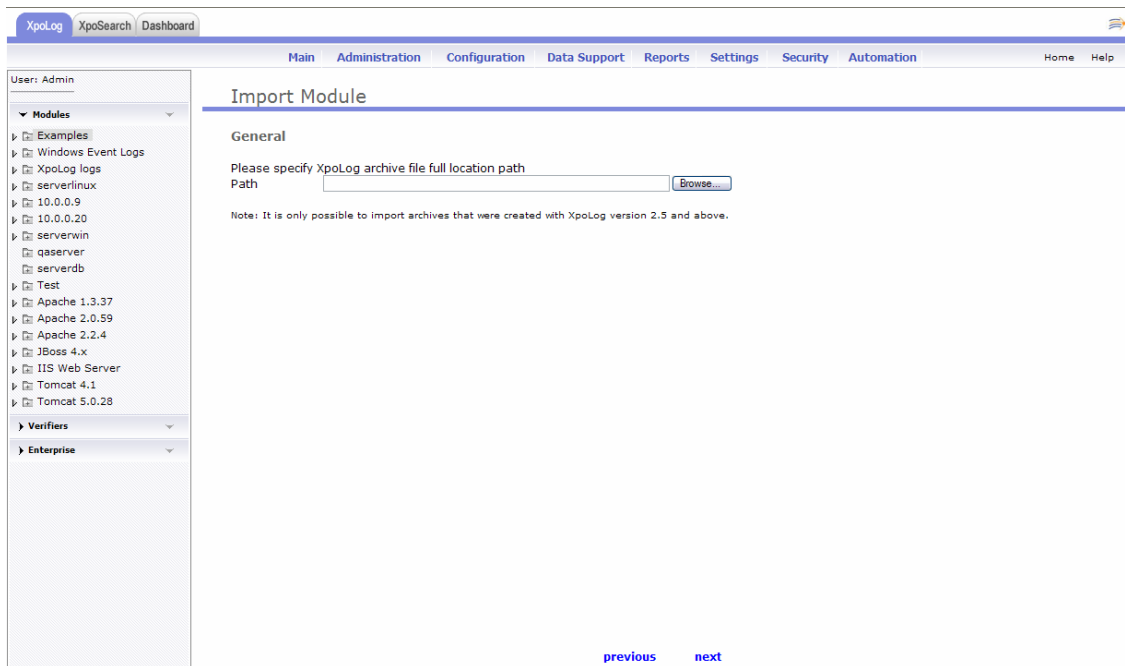
The module will be transferred over SSH to a remote machine. Select an SSH account from the list of available SSH accounts, or click new in order to configure a new SSH account. For further information regarding SSH accounts, please refer to Data Support → Address book.

Specify the directory on the remote machine, in which XpoLog will copy the module to.

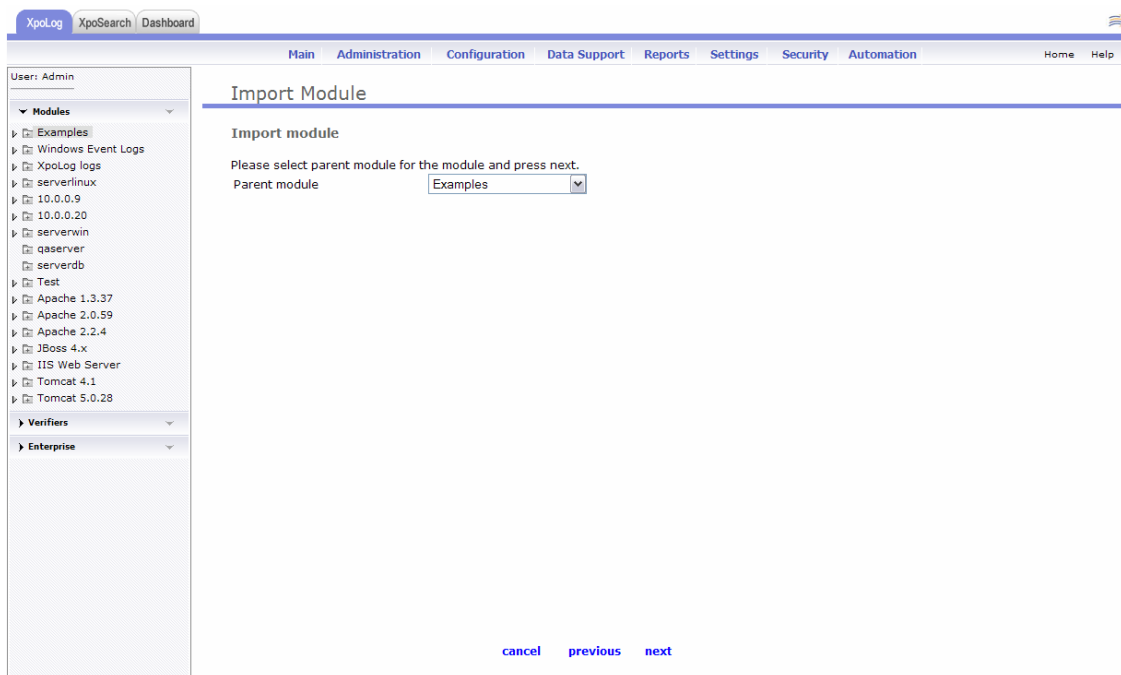
Click 'next' to start the transfer over SSH process.



Import module



In order to import a module to XpoLog, select ‘Import module’ from the data support menu. Specify the module’s path, and click ‘Next’



After locating the desired module, please select a parent module from the list of available modules. Click 'next' to finish the import process or 'previous' in case you would like to import a different module. Click 'Ok' to confirm the successful import.

Import configuration image

Importing a configuration image will update a vast part of XpoLog's components, according to the specific saved image.

In order to import a configuration image, select 'Import configuration image' from the Data support menu.

For further information on how to save a configuration image, please refer to Configuration → Configuration image.

User: Admin

Navigation: Main Administration Configuration Data Support Reports Settings Security Automation Home Help

Left Sidebar:

- Modules
 - Examples
 - Windows Event Logs
 - XpoLog logs
 - serverlinux
 - 10.0.0.9
 - 10.0.0.20
 - serverwin
 - qaserver
 - serverdb
 - Test
 - Apache 1.3.37
 - Apache 2.0.59
 - Apache 2.2.4
 - JBoss 4.x
 - IIS Web Server
 - Tomcat 4.1
 - Tomcat 5.0.28
- Verifiers
 - Enterprise

Main Content:

update configuration from image

Location

Please specify the file containing the configuration image

Path

Note: importing the configuration file results in updating your modules and logs.

Navigation: [previous](#) [next](#)

Specify the path where the saved image is located, and click ‘Next’.

While XpoLog is importing the configuration image, a message will be displayed,

Import Configuration

Please wait...

Importing the configuration file might take a couple of minutes.

indicating that the import process might take a few minutes.

When XpoLog finished importing the configuration image, all accounts from the image that has no password will be displayed. Click each account name, and specify its password in order to be able to use it in XpoLog. Saving the account’s properties will lead you back to the import image wizard. When done setting passwords to all accounts, click ‘OK’ in order to finish the import image process.

Please Notice.

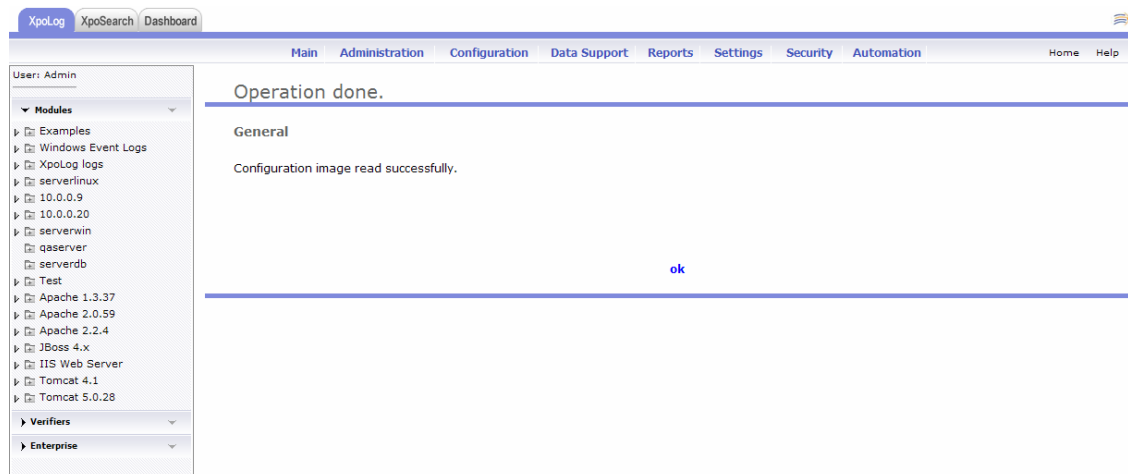
The following accounts have no passwords! Please set new passwords.

Name	Type	Description
PostgreSQL	db	
auth xplg	winAuthentication	
ssh xpolog@10.0.0.20	ssh	
SQL Server	db	
default SQL DB	db	
ssh xplg@10.0.0.9	ssh	
ssh root@10.0.0.9	ssh	
MySQL	db	
Oracle	db	
ssh root@serverlinux	ssh	
FTP	ftp	
FTP	ftp	
ssh root@serverlinux	ssh	
auth xplg	winAuthentication	
ssh root@10.0.0.9	ssh	
ssh root@serverlinux	ssh	

cancel

ok

A message indicating that the new configuration image was successfully imported will be displayed. Click 'OK' to finish the import wizard.



Email text

XpoLog allows you to send a log's content by email. While the specific log is in focus (In

The screenshot shows the 'email current text' dialog box in the XpoLog application. The interface includes a top navigation bar with tabs for 'XpoLog', 'XpoSearch', and 'Dashboard'. Below this is a menu bar with options: 'Main', 'Administration', 'Configuration', 'Data Support', 'Reports', 'Settings', 'Security', 'Automation', 'Home', and 'Help'. On the left, a sidebar shows a tree view of modules, including 'Examples', 'Windows Event Logs', 'XpoLog logs', 'serverlinux', '10.0.0.9', '10.0.0.20', 'serverwin', 'qaserver', 'serverdb', 'Test', 'Apache 1.3.37', 'Apache 2.0.59', 'Apache 2.2.4', 'JBoss 4.x', 'IIS Web Server', 'Tomcat 4.1', and 'Tomcat 5.0.28'. The main area is titled 'email current text' and contains a note: 'Note: if you want to use your default mail client [click here](#) and copy/paste the text into it. XpoLog can not do this for you due to browser constraints. Sorry.' Below the note are input fields for 'From' (sender email), 'To' (recipient(s) email), and 'Subject' (pre-filled with 'XpoLog mail - XpoAudit log'). There is also a 'Text' input area. A 'Log text' section displays a list of log entries, including timestamps, IP addresses, and system messages. At the bottom, there are 'Cancel' and 'Send' buttons, and a small disclaimer: 'Only the text will be added to the message. New text in the log filed will be ignored.'

the log viewer) select the 'Email text' option from the Data Support menu.

Specify the sender's and recipient email. The default subject would be 'XpoLog mail – the name of the log', but you may change it, and add a text to the email as well.

Click 'Send' when done, or cancel to discard the email.

Address book

Address Book

View addresses from type All

[Add new Account](#)

Name	Description	Type
cancel		

In order to create new accounts click the ‘Add new Account’ link.

Accounts List

Please choose the type of Account

Name	Description
Database Account	Add a new database account
File System Account	Add a new file system account
Ftp Account	Add a new ftp account
Http Account	Add a new http account
Email Account	Add a new email account
Ssh Account	Add a new ssh account
SNMP Account	Add a new SNMP account
JMS Account	Add a new JMS account
Win Authentication Account	Add a new Windows authentication account

[previous](#) [cancel](#)

Database Account

1. Click the ‘Database Account’ link from the ‘Accounts List’ page.

Databases List

Please choose the type of Database

Name	Description	Driver Name	Version	JDBC driver	
hsqldb	Driver To hsqldb	org.hsqldb.jdbcDriver		available	download
PostgreSQL	Driver To PostgreSQL db	org.postgresql.Driver		n/a	download
Interbase	Driver To Interbase db	interbase.interclient.Driver		n/a	download
Odbc	Connector to odbc data source	sun.jdbc.odbc.JdbcOdbcDriver		available	
SQL Server	Driver To SQL Server db	com.microsoft.jdbc.sqlserver.SQLServerDriver		n/a	download
DB2	Driver To DB2 db	COM.ibm.db2.jdbc.app.DB2Driver		n/a	download
Oracle	Driver To Oracle DB	oracle.jdbc.driver.OracleDriver	8.1.7	n/a	download
Other	General DB driver definition	N/A		n/a	
MySQL	Driver To MySQL DB	com.mysql.jdbc.Driver	3.0.9	n/a	download
Data Source	Data source to database			n/a	

[previous](#) [upload driver](#) [cancel](#)

2. Choose the database type and specify the following configuration details (not all fields apply to all database types):
 - **Name:** the name of the new account.
 - **Description (optional):** the description of the new account.
 - **Driver Name:** filled in automatically.

- **User Name:** the username used to connect to the database.
- **Password (optional):** the password used to connect to the database.
- **Database Name:** the name of the database to connect to.
- **Machine Address:** the address of the machine on which the database is installed.
- **Port:** the port on which the database accepts connections.
- **Connection string params (optional):** parameters that should be passed upon connection.

If you choose to add a Data Source (and not define a database account), you should specify the following configuration details:

- **Name:** the name of the data source.
- **Description (optional):** the description of the data source.
- **JNDI Name:** the JNDI name of the data source.
- **Environment Properties (optional)**
- **Database Type:** select the type of database the data source will work against (choose 'other' for an unknown database).

3. Click 'save' to save the new account.

File System Account

1. Click the 'File System Account' link from the 'Accounts List' page.

File System Account

File System details

Name	<input type="text"/>
Description	<input type="text"/>
Path	<input type="text"/>

cancel save

2. Specify the following configuration details:
 - **Name:** the name of the new account.
 - **Description (optional):** the description of the new account.
 - **Path:** the path in the file system the account points to.
3. Click 'save' to save the new account.

FTP Account

1. Click the 'Ftp Account' link from the 'Accounts List' page.

FTP Account

FTP details

Name	<input type="text"/>	
Description	<input type="text"/>	
Host Address	<input type="text"/>	(ftp site url)
Port	<input type="text" value="21"/>	
User	<input type="text"/>	(ftp user name)
Password	<input type="text"/>	(ftp user password)

[cancel](#) [save](#)

2. Specify the following configuration details:
 - **Name:** the name of the new account.
 - **Description (optional):** the description of the new account.
 - **Host Address:** the host name/IP address of the FTP site.
 - **Port:** the port on which the FTP server accepts connections.
 - **User:** the username used to connect to the FTP server.
 - **Password:** the password used to connect to the FTP server.
3. Click 'save' to save the new account.

HTTP Account

1. Click the 'Http Account' link from the 'Accounts List' page.

HTTP Account

HTTP details

Name	<input type="text"/>	
Description	<input type="text"/>	
Host URL	<input type="text"/>	(http/s site url)

[cancel](#) [save](#)

2. Specify the following configuration details:
 - **Name:** the name of the new account.
 - **Description (optional):** the description of the new account.
 - **Host URL:** the URL the account points to.
3. Click 'save' to save the new account.

Email Account

1. Click the 'Email Account' link from the 'Accounts List' page.

eMail Account

eMail details

Name	<input type="text"/>
Description	<input type="text"/>
eMail address	<input type="text"/>

Note: address may contain multiple entries seperated by a semicolon (";")

[cancel](#) [save](#)

2. Specify the following configuration details:
 - **Name:** the name of the new account.
 - **Description (optional):** the description of the new account.
 - **eMail address:** the email address to be used by the account.
3. Click 'save' to save the new account.

Ssh Account

1. Click the 'Ssh Account' link from the 'Accounts List' page.

SSH Account

SSH details

Name	<input type="text"/>	
Description	<input type="text"/>	
Host Address	<input type="text"/>	(SSH machine url)
Port	<input type="text" value="22"/>	
User	<input type="text"/>	(Ssh user name)
Password	<input type="password"/>	(Ssh user password)

☐ SCP Connection Type is Secure Copy (default: SFTP)

[cancel](#) [save](#)

2. Specify the following configuration details:
 - **Name:** the name of the new account.
 - **Description (optional):** the description of the new account.
 - **Host Address:** the host name/IP address of the remote host.
 - **Port:** the port on which the remote host accepts SSH connections.
 - **User:** the username to be used to connect to the remote host.

- **Password:** the password to be used to connect to the remote host.
 - **SCP:** check if the remote host does not support SFTP for file transfer.
3. Click 'save' to save the new account.

SNMP Account

1. Click the 'SNMP Account' link from the 'Accounts List' page.

SNMP Account

SNMP details

Name	<input type="text"/>
Description	<input type="text"/>
Host	<input type="text"/>
Port	<input type="text"/>
Version	<input type="text" value="Version 2"/>
Protocol	<input type="text" value="UDP"/>

[cancel](#) [save](#)

2. Specify the following configuration details:
 - **Name:** the name of the new account.
 - **Description (optional):** the description of the new account.
 - **Host:** the host name/IP address of the remote host.
 - **Port:** the port on which the remote host accepts SNMP traps.
 - **Version:** the version of SNMP to be used.
 - **Protocol:** the protocol to be used.
3. Click 'save' to save the new account.

JMS Account

1. Click the 'JMS Account' link from the 'Accounts List' page.

JMS Account

JMS details

Name	<input type="text"/>
Description	<input type="text"/>
JNDI Context	<input type="text" value="org.exolab.jms.jndi.InitialContextFactory"/> <small>Enter the full path to the JNDI context. Mandatory.</small>
JNDI Provider URL	<input type="text" value="tcp://localhost:3035"/> <small>Mandatory.</small>
User Name	<input type="text" value="admin"/> <small>May be null.</small>
Password	<input type="password" value="••••••"/> <small>May be null.</small>
JMS Topic Factory	<input type="text" value="JmsTopicConnectionFactory"/> <small>Mandatory.</small>
JMS Queue Factory	<input type="text" value="JmsQueueConnectionFactory"/> <small>Mandatory.</small>

[cancel](#) [save](#)

2. Specify the following configuration details:
 - **Name:** the name of the new account.
 - **Description (optional):** the description of the new account.
 - **JNDI Context:** the full JNDI context.
 - **JNDI Provider URL:** the URL to be used to access the JNDI provider.
 - **User Name:** the username to be used to connect to the JNDI provider.
 - **Password:** the password to be used to connect to the JNDI provider.
 - **JMS Topic Factory:** the JNDI name of the JMS topic factory.
 - **JMS Queue Factory:** the JNDI name of the JMS queue factory.
3. Click 'save' to save the new account.

Win Authentication Account

1. Click the 'Win Authentication Account' link from the 'Accounts List' page.

Windows Authentication Account

Account details

Name	<input type="text"/>	
Description	<input type="text"/>	
User	<input type="text"/>	(user name)
Password	<input type="password"/>	(user password)

[cancel](#) [save](#)

2. Specify the following configuration details:
 - **Name:** the name of the new account.
 - **Description (optional):** the description of the new account.
 - **User:** the username of the Windows Authentication account.
 - **Password:** the password of the Windows Authentication account.
3. Click 'save' to save the new account.

Enterprise

XpoLog Enterprise Cloud

Search

go reset

Add Remote XpoLog

Name	Description	Location	Type
------	-------------	----------	------

cancel

In order to create new remote XpoLogs click the ‘Add Remote XpoLog’ link.

Remote XpoLog Connection

General details

Name

Description

Host name

Protocol

Http port

URL context

Remote XpoLog address

HTTP

Remote XpoLog Protocol Http/s

30303

Remote XpoLog Http/s port

logeye

Remote XpoLog web context (default: logeye)

Remote registration details

Current host

10.0.0.39

Add current XpoLog according to this address in the remote host

Security details

Auto Login

User Name

Password

☐ check for auto login, uncheck to force manual login

cancel

save

Specify the following configuration details:

1. General details

- **Name:** the name of the remote XpoLog.
- **Description (optional):** the description of the remote XpoLog.
- **Host name:** the host name/IP address the remote XpoLog is running on/
- **Protocol:** the protocol allowed by the remote XpoLog.
- **Http port:** the port on which the remote XpoLog is listening.
- **URL context:** the context of the remote XpoLog.

2. Remote registration details

- **Current host:** the host name/IP address to be used for the XpoLog node representing the current host that will be added in the remote XpoLog.

3. Security details

- **Auto Login:** when checked, no prompt for username and password will appear when accessing the remote XpoLog.
 - **User Name:** the username to be used to access the remote XpoLog.
 - **Password:** the password to be used to access the remote XpoLog.
4. Click the 'save' link to save the new remote XpoLog.

After a remote XpoLog was added you can click its name to access it.

You can search remote XpoLog nodes by entering a search term in the 'Search' text box and clicking the 'go' link. Clicking the 'reset' link will display all remote XpoLogs that were added to the system.

Meta Data

Meta data List

[add new](#)

Name	Description
------	-------------

[ok](#)

In order to create new metadatas click the ‘add new’ link.

Meta data settings

General settings

Id

Name

Description

Properties

Application

— select —

Version

Build

Platform

PC
Mec
AS/400
IBM RS6000
other

Operating system

Windows
OS/2
Linux
OS X
other

Vendor

— select —

[add new property](#)

Search Context Menu

Name

Path

[Add Menu](#)

[cancel](#)

[save](#)

Specify the following details:

1. General settings

- **Id:** the id of the new metadata.
- **Name:** the name of the new metadata.
- **Description (optional):** the description of the new metadata.

2. Properties

- **Application (optional):** the application type of the new metadata.
- **Version (optional):** the application version of the new metadata.
- **Build (optional):** the application build of the new metadata.
- **Platform (optional):** the platform of the new metadata. Choose other to specify a custom platform.

- **Operating system (optional):** the operating system of the new metadata.

Choose other to specify a custom operating system.

- **Vendor (optional):** the vendor of the new metadata.

Click the 'add new property' link to add custom properties. Specify the type and value of each custom property.

3. **Search Context Menu**

Click the 'Add Menu' link to add custom search context menus. Specify the name and path of each custom menu.

Click the 'save' link to save the new metadata.

Reports

Report Definition

Reports Definition

Add new Report

Name

Description

cancel

This page shows all the reports in the system, grouped by the applications (metadata) they belong to. Reports that are not associated with any application are all grouped under 'Other'. Click the arrow next to an application to display its reports.

In order to add a new report definition click the 'Add new Report' link in the 'Reports Definition' page. After clicking the link the following page will appear:

Aggregation Report Definition

General

Name:

Aggregation

Description:

Data Distribution

☐ None

☒ Automatic

☐ Over days

☐ Over hours

☐ Over minutes

Time Filter

☒ Dates limit

☐ Show records that arrive after

08/02/2007 16:57:57

calendar

(MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH:mm:ss:SSS)

☐ Show records that arrive before

08/02/2007 16:57:57

calendar

(MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH:mm:ss:SSS)

☐ show records

from the last

minutes

Status

Failure means that there are

at least one case failed

next

back to reports view

1. General

Enter the new report's name and description.

2. Data Distribution

Select the data unit for which aggregation data will be computed (you can override this setting when you generate a new report runtime):

- None: no computation of data distribution will take place. an empty cases distribution graph will be displayed

- Automatic: XpoLog sets automatically the data units either to 'hours' or 'days', according to the time span of the different data sources
- Over days: data will be aggregated for each day
- Over hours: data will be aggregated for each hour
- Over minutes: data will be aggregated for each minute

3. Time Filter

Define default time constraints for the report generation (you can override this setting when you generate a new report runtime).

You can define time constraints in two ways:

- Selecting the 'Dates limit' option and entering the minimum and/or maximum date.
- Selecting the 'show records' option. in the following combo box select one of the following options:
 - from the last: defines a time interval that starts with the specified time constraint and stretches until the current time
 - from the previous: defines a time interval that contains only the specified days, weeks or months
 - from: defines a time interval the starts in the data specified in number text field and time unit (in the case of 'days' a starting hour is required too) and stretches for the time span defined in the 'for' section of the filter

4. Status

Select the logic by which the report's status will be determined:

- Select 'at least one case failed' in order to set the report status to 'failed' when at least one case/dimension has failed.
- Select 'all cases failed' in order to set the report status to 'failed' when all of the report's cases/dimensions have failed.

5. Click 'next' to continue to defining the report's cases and dimensions (columns).

Define a new report case

1. Click 'Add new aggregation rule' to create a new case.

Log Case Selection

General

Name:

Description:

Logs List

Select a log to be used in this case

Select from used logs:

- ▼ Modules
- ▶ Examples

[cancel](#) [previous](#) [next](#)

2. General

- Enter the new case's name and description. If you leave the default description 'LOG_NAME [FILTERS_NAME]', XpoLog will replace in the created report 'LOG_NAME' with the name of the selected log and 'FILTERS_NAME' with the name of the selected filter(s).

3. Logs List

- Select the log to be used for the case. You can either select a log from the logs tree or select a previously selected log from the 'Select from used logs' combo box.

4. Click 'next' to continue to selecting filters to be included in the case.

Log Case - Fields

Status

☐ Failure means that there are more than 0 records in the result.

Data Filters

Data Filters		Show only
Error	add add all remove remove all	

[previous](#) [next](#)

5. Status

- Click on the check box to turn on the computation of the case's status. Select 'more than' or 'less than' and enter the number of records in the result to complete the definition of the case's status. If the checkbox is left unchecked, no status for that case will be computed.

6. Data Filters

- Select the filters to be included in the case.

7. Click 'next' to continue adding the report's cases.

8. Repeat steps 1 to 7 to add more cases.

9. Click 'save' when finished adding the report's cases and dimensions.

Define a new report dimension (column)

1. Click 'Add new column aggregation' to create a new dimension.

Log Column Aggregation

General

Name:

Description:

Logs List

Select a log to be used in this dimension

Select from used logs:

- ▼ Modules
- ▶ Examples

[cancel](#) [previous](#) [next](#)

2. General

- Enter the new case's name and description. If you leave the default name 'COLUMNS_NAME Aggregation' and description 'LOG_NAME [COLUMNS_NAME]', XpoLog will replace in the created report 'LOG_NAME' with the name of the selected log and 'COLUMNS_NAME' with the name of the selected column.

3. Logs List

- Select the log to be used for the dimension. You can either select a log from the logs tree or select a previously selected log from the 'Select from used logs' combo box.

4. Click 'next' to continue to selecting columns and filters to be included in the dimension.

Log Column Aggregation - Column

Column aggregation

Select a column to be aggregate.

Data Filters		Show only
<div>Date Thread Priority Logger Code Message</div>	<div>add add all remove remove all</div>	<div></div>

Data Filters

Select the records you want to aggregate.

Data Filters		Show only
<div>Error</div>	<div>add add all remove remove all</div>	<div></div>

Table Display Settings

- ☒ Display all results
- ☐ Display top results
- ☐ Don't display table

Status

☐ Failure means that there are records in the result.

[previous](#) [next](#)

5. Column aggregation

- Select the log's column to be aggregated.

6. Data Filters

- Select the filters to be included in the dimension.

7. Table Display Settings

- Set the number of results to be displayed in the column section of the report runtime result:
 - Select 'Display all results' to show all distinct values (XpoLog collects only the top 5000 distinct values).
 - Select 'Display to X results' and specify the number of distinct values to be displayed.
 - Select 'Don't display table' to display only a graph.

8. Status

- Click on the check box to turn on the computation of the dimension's status. Select 'more than' or 'less than' and enter the number of records in the result to complete the definition of the dimension's

status. If the checkbox is left unchecked, no status for that dimension will be computed.

9. Click 'next' to continue adding the report's dimensions.
10. Repeat steps 1 to 9 to add more dimensions.
11. Click 'save' when finished adding the report's cases and dimensions.

Report Generation

Reports Definition

Add new Report

Name

↳ other

Aggregation

Description

cancel

edit verifier delete generate

1. Click 'generate' or click the report name to enter the 'Reports Runtime' page and click the 'Generate new report runtime' link.

Aggregation Report Definition

General

Name:

Aggregation

Description:

Data Distribution

☐ None

☒ Automatic

☐ Over days

☐ Over hours

☐ Over minutes

Time Filter

☒ Dates limit

☐ Show records that arrive after

08/04/2007 00:40:22

calendar

(MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH

☐ Show records that arrive before

08/04/2007 00:40:22

calendar

(MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH

☐ show records

from the last

minutes

Status

Failure means that there are at least one case failed

generate

back to reports view

2. The 'Data distribution' and the 'Time Filter' are taken from the report definition. You can override these values for each report execution.
3. Click 'generate' to generate the report.

Report Verifier

Reports Definition

[Add new Report](#)

Name	Description
other	
Aggregation	cancel edit verifier delete generate

1. Click 'verifier'.

Report Verifier Settings

Global

Name:

Actions

execute following actions upon verifier **success**:

Actions		Execute actions
<input type="text"/>	add add all remove remove all	<input type="text"/>

execute following actions upon verifier **failure**:

Actions		Execute actions
<input type="text"/>	add add all remove remove all	<input type="text"/>

[show advanced options](#)

[save](#) [reset](#) [cancel](#)

2. **Global**

- o Enter the name of the report verifier.
- o Select the actions to take place upon verifier success and failure.

3. Click 'save' to save the verifier.

Settings Menu

License

Settings

License(You can paste a new license and save it)

Licensee	<input type="text" value="Xpolog"/>
Version	<input type="text" value="3.0"/>
Update	<input type="text" value="false"/>
Max Logs	<input type="text" value="5000"/>
Max Data Sources	<input type="text" value="1000"/>
Feature	<input type="text"/>
Components	<input type="text" value="XpoLog,SearchEngine,Dashboard,TransactionExpo"/>
Permanent	<input type="text" value="true"/>
Expiration	<input type="text" value="2007-6-19"/>
Signature	<div><div></div><div></div></div>

[cancel](#) [save](#)

This page is used to update the license of XpoLog.

In order to update your license, execute the following steps:

Open the license.lic file that contains your license details.

Paste the value of each filed in the appropriate location.

Click the 'save' link.

Operation verification.

General

Are you sure you want to save the license:

MaxLogs=5000
Feature=
Licensee=Xpolog
Version=3.0
Licensor=Xpolog
Permanent=true
Expiration=2007-6-19
Update=false
MaxDataSources=1000
Components=XpoLog,SearchEngine,Dashboard,TransactionExpo

[cancel](#) [Previous](#) [ok](#)

Verify the license details and click the 'ok' link to confirm.

Settings → General

General settings

Mail - SMTP

SMTP host

mail.xplg.com

(example: mail.mydomain.com)

SMTP port

25

(default: 25)

Ports

Http Port

30303

(default: 30303)

SSL Port

30443

(default: 30443)

XpoLog Configuration directory

☐ Use external configuration directory

Set here an external full path where XpoLog will save and load the configuration files and directories.
Recommended for Clustered environment, or when deploying XpoLog as a web application.
Note: you must restart XpoLog in order for the changes to take effect.

Configuration full path

---check the use external configuration to set the path---

☐ Cluster mode

If checked, XpoLog will run in cluster mode, enabling sharing of the external configuration
by different server instances and making one instance a master

Security

Activate security

☐ (Show login page for new connections)

Session time out

30

(default: 30 minutes)

Default SSL

☐ (open secure line upon server initialization)

Login URL

security/auth/login.jsp

(every user will be redirected to this URL to validate login)

Authentication

Select the authentication types to be used:

Available Types

XpoLog Realm

Ldap

Siteminder

Remote User

Add

Remove

Selected Types

XpoLog Realm

XpoLog Realm

Configuration

XpoLog Realm: User and password is authenticated with XpoLog realm.

cancel

save

This page is used to update XpoLog's general settings. When you are finished updating the settings click the 'save' link for the changes to take effect.

- **Mail - SMTP**

Use this section to configure the SMTP host and port XpoLog should use to send emails.

- **Ports**

Use this section to configure the HTTP and HTTPS ports XpoLog will be listening on.

- **External Configuration**

you may save the entire configuration that XpoLog is using in a specific location.

To do so, execute the following steps:

1. Click the 'Use external configuration directory' check box.
2. Specify the path in which you XpoLog's configuration to be saved in the 'Configuration full path' text box.

3. If you want XpoLog to run in cluster mode, check the 'Cluster mode' check box.

Note that changing this setting requires performing a restart of XpoLog.

- **Security**

Use this section to configure XpoLog's security settings. The following settings are available:

1. Activate security - you can activate XpoLog's security mechanism by clicking the 'Activate security' check box. **Note** that after activating the security mechanism and clicking the 'save' link you will be redirected to XpoLog's login page, where you will be asked to enter a username and password to access XpoLog. In addition, a new menu, 'Security', will be added to XpoLog's top menu.
2. Session time out – use this setting to configure the session timeout period (in minutes). The default session timeout period is 30 minutes.
3. Default SSL – use this setting to redirect XpoLog's users to a secure channel (SSL) by default.
4. Login URL – use this setting to configure the URL to which users will be redirected for login.

- **Authentication**

Currently, XpoLog provides 4 different pre defined authentications types:

XpoLog realm, Active Directory/LDAP, Siteminder and Remote user.

Various different authentication methods have been successfully implemented in XpoLog over the past few years. In case your company uses a different authentication method then the one in the available types, please contact our support team for further assistance.

Both the LDAP and the Siteminder authentication methods should be configured before use.

Active Directory/LDAP Configuration:

Select LDAP from the table on the left ('Available types'), and add it to the 'Selected types' table. Click the 'LDAP configuration' link:

LDAP settings

General

Initial context factory

com.sun.jndi ldap.LdapCtxFactory

(example: com.sun.jndi ldap.LdapCtxFactory)

Provider url

ldap://localhost:389/

(example: ldap://localhost:389/)

Manager Settings

Manager path

(Empty for no authentication)

Manager password

(Empty for no password authentication)

Search Settings

Root path

(Empty for top root path)

Search filter

uid={0}

(Empty for no search. example: uid={0} ,where {0} will be replaced with username)

User path

(Empty for no user path)

Unique id attribute

(Empty for no search users. example: uid)

Display name attribute

(Empty for no display name attribute)

Further Settings

Group id pattern

(Empty for no group id. example: cn={0} ,where {0} will be replaced with group id)

cancel

save

- General:

Initial context factory – you may leave as default.

Provider URL – set the connection URL to the LDAP server.

Manager Settings (this is optional):

Manager Path – the manager DN for searching users.

Manager password – the manager’s password.

Search Settings:

Root Path – the path for start searching users.

Search Filter – how to search the users in the LDAP directory (the {0} is replaced with user name).

User Path- full path of the user DN (the {0} is replaced with user name). For example: uid={0},ou=people,cn=xplg

Unique Id – optional, which attribute of the user will be provided as the unique id of the user.

Display name attribute – optional, which attribute of the user will be provided as the display name of the user.

Save the LDAP configuration, and save the general settings configuration.

XpoLog will then authenticate users with the LDAP server.

Siteminder Configuration:

Siteminder settings

General

User header key

HTTP_SM_USER,SM_USER

(example: HTTP_SM_USER)

Client cookie name

SMSESSION

Protected URLs

URL's which are protected by the web agent, seperated by ','
wildcards are allowed

Group header key

Group id pattern

(example: c={0} ,where {0} will be replaced with group id)

cancel

save

- Click the Siteminder Configuration link in order to configure it:
In order to set more header key for retrieving the user information which was authenticated, you may use ‘,’ as a separator between parameters. For Example: HTTP_SM_USER, HTTP_UID – in this case XpoLog will look for the user first in the HTTP_SM_USER header key, and then if not found in the HTTP_UID header key.
You may use as many keys as you wish.
- Save the Siteminder configuration, and save the general settings configuration. XpoLog will then associate users in XpoLog according to Siteminder’s authentication.

Updates

Updates check result

Update unavailable

Installed version is2.8

Available version is2.8

Get updates from [XpoLog downloads page](#)

cancel

This page is used to check if there is a newer version of XpoLog available for download from XpoLog's download page.

UI Settings

UI Settings Center

Welcome to XpoLog's UI center. In this page you will find explanations and examples of how to edit XpoLog's skin. You have the following options:

Note: If you choose not to edit some or all of the above, XpoLog will use it's default definitions.

CSS definition

In this section you can edit the css files of XpoLog.
If you wish to edit the CSS, follow this link: [Edit CSS File](#)

Images Settings

In this section you can replace XpoLog's images.
If you wish to edit the images definitions, follow this link: [Edit Images](#)

This page is used to change the look and feel of XpoLog. The available changes are:

CSS definition:

Click the 'Edit CSS File' to read an explanation on how the CSS files can be edited.

XpoLog's CSS files resides in XpoLogInstallationDir\defaultroot\logeye\css

Edit Images:

click the 'Edit Images' link to specify new paths for images you wish to replace.

151

Log View Settings

Log View settings

Default Log Search Settings

Default Search

☒ When checked - a search and filter result will be presented from the beginning of the logs
(Note: when unchecked the result that will be presented is on current view)

Default Tail Settings

Tail refresh rate

2

you can set the refresh rate of tailing (in seconds)
(Note: when activating the tail on log view XpoLog is loading the new records according to the specified refresh rate)

Tail number of record view

500

while tailing XpoLog will accumulate the selected number of records in log view
(Note: after the view will reach the selected number of records, XpoLog will restart the accumulation)

Search Context Menu

Name	Path	
XpoSearch	javascript:searchText("search/search.jsp?searchTerm=[LOG_COL_DATA]	Add Menu remove
Google	http://www.google.com/search?hl=en&q=[LOG_COL_DATA]	remove

[cancel](#) [save](#)

This page is used to update settings common to all log views. The available settings are:

- **Default Log Search Settings**

checking the 'Default Search' check box will cause searches to be performed from the beginning of a log. Leaving it unchecked will cause searches to be performed from the current position.

- **Default Tail Settings**

This section controls the configuration of the tail feature. The available settings are:

- Tail refresh rate: specify the number of seconds between each tail refresh action. The default refresh rate is 2 seconds.
- Tail number of record view: specify the number of records that will be accumulated in the log view before switching to a new page. The default number of records is 500.

- **Search Context Menu**

it is possible to define a search context menu to enable search of logged data in data repositories, such as search engines and wikis.

Add a search context menu to all logs by specifying the name of the data repository (i.e. Google) and the URL to be used for the search.

Note that the URL can contain place holders for dynamic text replacement during the search.

System Audit

System Audit settings

Enable/Disable System Audit

System Audit

☒ When checked - the system will generate audit reports

Audit Settings

Select Audit Level

Basic Audit Level

set the level of audit the system will generate. Default valuse is basic audit.

Audit Types

set the types of audit reports. Leave empty or check all to include all audit reports types.

☒ Logins/Logouts

☒ View system components

☒ Change system components

cancel

save

This page is used to configure XpoLog's audit settings. The available settings are:

- **Enable/Disable System Audit**
Click the 'System Audit' check box to enable or disable system audit.
- **Audit Settings**
Use the 'Select Audit Level' combo box to specify the level of audit you wish XpoLog to produce.
- **Audit Types**
 - Logins/Logouts: when checked, users' login and logout operations will be audited.
 - View system components: when checked, users' viewing operations will be audited.
 - Change system components: when checked, users' editing operations will be audited.

Environment Variables

XpoLog environment settings

Environment variables

myServerLogsPath [remove](#)

[add new environment variable](#)

[cancel](#) [save](#)

This page is used to specify variables that can be user all across XpoLog. For example, you can add an environment variable that points to a logs folder, and in every log you add you only need to put the environment variable's name in the path, and not the full path. This way, if the path changes, you only need to edit the environment variable's value and all the logs will remain functional.

If the variable's name is **myServerLogsPath**, the value to be used in order to access it is **`${myServerLogsPath}`**

Note that after adding, editing or removing environment variables you must click the 'save' link for the changes to take effect.

Audit

System Audit

Time Frames

define the time frame of the audit view. Leave empty to run on all data.

☒ Dates limit

- ☐ Show records that arrive **after** [calendar](#) (MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH:mm:ss:SSS)
☐ Show records that arrive **before** [calendar](#) (MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH:mm:ss:SSS)

☐ show records from the last

Audit Types

Check the type of action you would like to view. Please select at least one type.

- ☒ Logins/Logouts
☒ View system components
☒ Change system components

General

User Name

enter a user name to generate a user related view. Leave empty to include all users.

General

enter a specific detail to be included in the view. For example: action type, component name, action description, etc. may be null.

[cancel](#) [generate](#)

This page is used to generate a filtered log view on audited data. The available filters are:

- **Time Frames**
specify the time frame of the audit view.
- **Audit Types**
specify the types of actions you wish to view.
- **General**
 - User Name: specify a user whose audit you wish to view.
 - General: specify a general term to be included in the filter, such as component name or action description.

After you are finished specifying the filter criteria click the 'generate' link to open the filtered audit log view.

About

Xpolog System Information

version: 3.0

patches

Version	Build	Deployment date	Description
---------	-------	-----------------	-------------

add patch

publish patch

ok

This page is used to view XpoLog's version and installed patches. The following actions are available:

- **Add patch**

click the 'add patch' link to add a patch to the system. The following page will appear:

Update from patch

Location

Please specify XpoLog patch file full location path

Path

Browse...

cancel

run

use the 'Browse' button to choose the patch and click the 'run' link to apply the patch.

- **Publish patch**

click the ‘publish patch’ link to distribute a patch to other XpoLog nodes that exist in your enterprise. The following page will appear:

Update from patch

To **start publishing**, select the file name of the patch to publish, check the XpoLog nodes you would like to publish it to and click next

Location

Please specify XpoLog patch file full location path

Path

Browse...

XpoLog Enterprise Nodes

Select the XpoLog Enterprise Nodes you want to publish the patch to
Displayed next to each node is it's status from the last publishing
[select all](#) [clear all](#)

☐ GALN

☐ Miron

☐ xplg6

☐ xplg8

cancel

run

use the ‘Browse’ button to choose the patch, choose the XpoLog nodes to which you want the patch to be published and click the ‘run’ link to publish the patch.

157

Security

User general settings

General User Settings

Global

Username:

admin

Password:

Display Name:

Admin

Save

Reset

Cancel

Use this page to change the password and display name of the current user.
Click the 'Save' link to apply the changes.

Users view

Users

Groups:

All

Group users

Add User

Name
Admin

View

Use the 'Groups' combo box to filter the users view by groups.
Click the 'Add User' link to create a new user.

User Settings

Global

Username:
Password:
Display Name:

Associated groups list

Select the groups to which this user is associated:

Available Groups		Associated Groups
Administrators All	Add Remove	

Administered groups list

Select the groups which this user administers:

Available Groups		Administered Groups
Administrators All	Add Remove	

Policy Settings

Select If the user will use the user's group policy or specific policy

- ☒ Use the policy of the selected groups
☐ Use the following policy:

[Save](#) [Reset](#) [Cancel](#)

Specify the following details of the new user:

Global

- **Username:** the username identifying the new user.
- **Password:** the password of the new user.
- **Display Name:** the name that will be displayed across the system.

Associated groups list: select the groups to which the user is associated.

Administration groups list: select the groups which the user administers.

Policy Settings: specify the policy to be associated with the user. Select from using the policy of the groups to which the user is associated or select a specific policy.

Click the 'Save' link to save the new user definition.

Groups view

Groups

Groups:

All

Groups members

Add Group

Name

Administrators

View

All

View

Use the 'Groups' combo box to filter the groups view by groups.

Click the 'Add Group' link to create a new group.

Group Settings

Global

Group name:

Display Name:

Description:

Groups list

Select the groups which this group Associated to:

Available Groups		Associated Groups
Administrators All Group A Group B	Add Remove	All

Administered groups list

Select the groups which this group administers:

Available Groups		Administered Groups
Administrators All Group A Group B	Add Remove	

Group Members

Select the groups members:

Available Members		Selected Members
Admin [user] Administrators [group] amir [user] Group A [group] Group B [group]	Add Remove	

Group Administrators

Select the groups administrators:

Available Members		Selected Members
Admin [user] Administrators [group] amir [user] Group A [group] Group B [group]	Add Remove	

Policy Settings

Select If the group will use the associated groups policy or specific policy

- ☒ Use the policy of the selected groups
- ☐ Use the following policy:

Save **Reset** **Cancel**

Specify the following details of the new group:

Global

- **Group name:** the name identifying the new group.
- **Display Name:** the name that will be displayed across the system.
- **Description (optional):** the description of the new group.

Groups List: select the groups which the group is associated to.

Administered Groups List: select the group which this group administers.

Group Members: select the users and groups that belong to the group.

Group Administrators: select the users and groups that administer the group.

Policy Settings: specify the policy to be associated with the group. Select from using the policy of the groups to which the group is associated or select a specific policy.

Click the 'Save' link to save the new group definition.

Policies view

Policies	
Policies	Add Policy
Name	
Administratinos	View
Default	edit

Click the ‘Add Policy’ link to create a new policy.

Policy Settings	
Global	
Policy name:	<input type="text"/>
Display Name:	<input type="text"/>
Description:	<input type="text"/>
Permissions List	
Select the actions to have permissions for the current policy:	
<input type="checkbox"/> All	
<input type="checkbox"/> XpoLog	
<input type="checkbox"/> Administration	
<input type="checkbox"/> Add Module	
<input type="checkbox"/> Remove Module	
<input type="checkbox"/> Edit Module	
<input type="checkbox"/> Add Log	
<input type="checkbox"/> Remove Log	
<input type="checkbox"/> Edit Log	
<input type="checkbox"/> Add Verify	
<input type="checkbox"/> Remove Verify	
<input type="checkbox"/> Edit Verify	

Specify the following details of the new policy:

Global

- **Policy name:** the name identifying the new policy.
- **Display Name:** the name that will be displayed across the system.
- **Description (optional):** the description of the new policy.

Permissions List: specify the permissions of the policy by choosing the components and allowed actions of each component. By leaving all check boxes unchecked a policy can define a view only permission for modules and logs and no permission for all other components in XpoLog.

Click the ‘Save’ link to save the new policy definition.

Automation Menu

Scheduler

Scheduler Tasks Book

View Jobs of type All

[Add new Job](#)

Name	Description	Type	Status
------	-------------	------	--------

[cancel](#)

In order to add a new scheduled job click the ‘Add new Job’ link in the ‘Scheduler Tasks Book’ page. After clicking the link the following page will appear:

Jobs List

Please choose the type of job

Name	Description
Verification Job	Add a new verifier job
Operation Job	Add a new operation job

[previous](#) [cancel](#)

Define a new Verification Job

1. Click the ‘Verification Job’ link.
2. Task Details

Verifier Task

Task details

Name

Description

Verifier

Error

☒ Activate root tasks

☐ Activate children tasks

- Enter the new scheduled task’s name and description.
- Select the verifier to be activated by the scheduler from the ‘Verifier’ combo box.

- Check the 'Activate root tasks' check box to enable the events mechanism of the selected verifier.
- Check the 'Activate children tasks' check box if you want the tasks of the children verifiers (in cases of multi verifiers which are based on other verifiers) to be executed as well.

3. Schedule Information

Schedule Information

Start at 08/05/2007 00:04:58 [calendar](#)

End at [calendar](#) [clear](#)

☒ Intervals

Repeat every minutes

Activate the task no more then iterations.

☐ Scheduling

☒ Activate at specific days every week

☐ Sun. ☐ Mon. ☐ Tues. ☐ Wed. ☐ Thurs. ☐ Fri. ☐ Sat.

☐ Activate at specific days in months

On month at day (s)

Activate on the given hour

On every scheduled day activate the task at

: : (hour:minutes:second)

Hours and minutes intervals

iterate every hours for each activation day

iterate every minutes for each activation hour

[cancel](#)

[save](#)

- Click on the 'calendar' link of the 'Start' definition to specify future scheduling.
- Click on the 'calendar' link of the 'End' definition to specify the end time or leave blank for unlimited executions.
- Specify the scheduling information in one of two ways:
 - **Intervals:** execute the job at specific time intervals. Enter the number of hours, minutes or seconds that determine the interval and select whether the operation should be run only a number of times or should be unlimited.

- **Scheduling:** select either the days of the weeks in which the execution should take place, or specify the days of the month and the desired months in which you want your job to run.

After defining the days at which your job should be executed define the time of desired executions. You can enter either a specific time (in the 'Activate on the given hour' section) or define hours interval and minutes interval (in the Hours and minutes intervals' section), so that on the selected days the operation will be executed in the given hours intervals and within each hour in the given minutes interval. For example, selecting in the scheduling section 'Every month' and 'Every day' and then defining to iterate every three hours and within each hour every 20 minutes will cause the job to be executed every at 00:20, 00:40, 01:00, 03:00, 03:20 and so on.

4. Click the 'save' link.

Scheduler Tasks Book

View Jobs of type
Verification

[Add new Job](#)

Name	Description	Type	Status	
Error Scheduler		verifier	Active	suspend edit run delete

[cancel](#)

After saving, the scheduled verification job it is automatically active and will be executed according to the specified schedule.

Click the 'suspend' link to cancel future executions. Click the 'activate' link to reschedule future executions.

Click the 'run' link to force a single execution of the scheduled job.

Define a new Operation Job

1. Click the 'Operation Job' link.
2. Task Details

General Task

Task details

Name	<input type="text"/>
Description	<input type="text"/>
Tasks	<input type="text" value="Zip Files"/>

- o Enter the new scheduled task's name and description.
- o Select the task to be activated by the scheduler from the 'Tasks' combo box.

3. Schedule Information

Schedule Information

Start at 08/05/2007 00:04:58 [calendar](#)
End at [calendar](#) [clear](#)

☒ Intervals

Repeat every minutes
Activate the task no more than iterations.

☐ Scheduling

☒ Activate at specific days every week

☐ Sun. ☐ Mon. ☐ Tues. ☐ Wed. ☐ Thurs. ☐ Fri. ☐ Sat.

☐ Activate at specific days in months

On month at day (s)

Activate on the given hour

On every scheduled day activate the task at
 : : (hour:minutes:second)

Hours and minutes intervals

iterate every hours for each activation day
iterate every minutes for each activation hour

[cancel](#) [save](#)

- o Click on the 'calendar' link of the 'Start' definition to specify future scheduling.

- Click on the 'calendar' link of the 'End' definition to specify the end time or leave blank for unlimited executions.
- Specify the scheduling information in one of two ways:
 - **Intervals:** execute the job at specific time intervals. Enter the number of hours, minutes or seconds that determine the interval and select whether the operation should be run only a number of times or should be unlimited.
 - **Scheduling:** select either the days of the weeks in which the execution should take place, or specify the days of the month and the desired months in which you want your job to run.
 After defining the days at which your job should be executed define the time of desired executions. You can enter either a specific time (in the 'Activate on the given hour' section) or define hours interval and minutes interval (in the Hours and minutes intervals' section), so that on the selected days the operation will be executed in the given hours intervals and within each hour in the given minutes interval. For example, selecting in the scheduling section 'Every month' and 'Every day' and then defining to iterate every three hours and within each hour every 20 minutes will cause the job to be executed every at 00:20, 00:40, 01:00, 03:00, 03:20 and so on.

4. Click the 'save' link.

Scheduler Tasks Book

View Jobs of type Verification

[Add new Job](#)

Name	Description	Type	Status	
Error Scheduler		verifier	Active	suspend edit run delete

[cancel](#)

After saving, the scheduled operation job it is automatically active and will be executed according to the specified schedule.

Click the 'suspend' link to cancel future executions. Click the 'activate' link to reschedule future executions.

Click the 'run' link to force a single execution of the scheduled job.

Tasks

Task Types

View tasks from type

[Add new Task](#)

Name	Description	Type
------	-------------	------

[cancel](#)

In order to add a new task definition, click the 'Add new Task' link.

Tasks List

Please choose the type of task

Name	Description
Execute Task	Add a new execute task
Remote Ssh command Task	Add a new execute task
URL Task	Add a new URL task
Email Task	Add a new email task
Export Module	Add a new export module task
JMS Message	Add a new JMS Message task
SNMP Trap	Add a new SNMP Trap task
General Report	Add a new general report generation task

[previous](#) [cancel](#)

Adding a new Execute Task

1. Click the 'Execute Task' link from the 'Tasks List' page.

Execute Task

Execution details

Name	<input type="text"/>
Description	<input type="text"/>
Program/Script path	<input type="text"/>
Arguments	<input type="text"/>
Environment variables	<input type="text"/>
Working directory	<input type="text"/>
Output target file	<input type="text"/>
Add optional params	<input checked="" type="checkbox"/> when checked the output file will contain the date, account name, host name and username

[cancel](#)

[save](#)

2. Specify the following configuration details:
 - **Name:** the name of the new task.
 - **Description (optional):** the description of the new task.

- **Program/Script path:** the name of the program/script to be executed by the task.
 - **Arguments (optional):** the arguments needed for the program/script to run, separated by spaces.
 - **Environment variables (optional):** the environment variables needed for the program/script to run.
 - **Working directory (optional):** the directory from which the program/script should be run.
 - **Output target file (optional):** the path to the file to which output of the program/script execution will be written.
 - **Add optional params:** check to include the date, account name, host name and username in the output file.
3. Click the 'save' link to save the new task definition.

Adding a new Remote Ssh command Task

1. Click the 'Remote Ssh command Task' link from the 'Tasks List' page.

Execute Task

Execution details

Name	<input type="text"/>
Description	<input type="text"/>
Ssh Account	--- Select Ssh account --- <input type="button" value="new"/>
Program/Script path	<input type="text"/>
Arguments	<input type="text"/>
Environment variables	<input type="text"/>
Output target file	<input type="text"/>
Add optional params	<input checked="" type="checkbox"/> when checked the output file will contain the date, account name, host name and username

[cancel](#)

[save](#)

2. Specify the following configuration details:
- **Name:** the name of the new task.
 - **Description (optional):** the description of the new task.
 - **Ssh account:** the account of the host on which the program/script will be executed.
 - **Program/Script path:** the name of the program/script to be executed by the task.
 - **Arguments (optional):** the arguments needed for the program/script to run, separated by spaces.

- **Environment variables (optional):** the environment variables needed for the program/script to run.
 - **Output target file (optional):** the path to the file to which output of the program/script execution will be written.
 - **Add optional params:** check to include the date, account name, host name and username in the output file.
3. Click the 'save' link to save the new task definition.

Adding a new URL Task

1. Click the 'URL Task' link from the 'Tasks List' page.

URL Task

URL details

Name	<input type="text"/>
Description	<input type="text"/>
Http Account	localhost <input type="button" value="new"/>

[cancel](#)
[save](#)

2. Specify the following configuration details:
- **Name:** the name of the new task.
 - **Description (optional):** the description of the new task.
 - **Http account:** the account on which the program/script will be executed.
3. Click the 'save' link to save the new task definition.

Adding a new Email Task

1. Click the 'Email Task' link from the 'Tasks List' page.

eMail Task

Details

Name	<input type="text"/>
Description	<input type="text"/>
From	<div><div>--- Select email account ---</div><div>new</div></div>
To	<div><div>--- Select email account ---</div><div>new</div></div>
Subject	<input type="text"/>
Body	<div><div></div></div>

Data Export Format

XpoLog can export the filtered data in several formats. XpoLog will attach a file with the transformed data (if found) after applying the filter.

In order not to export any data with the email, choose the first option.

- ☒ Send an email alert without any data attached
- ☐ Attach the log together with its configuration, to enable future import
- ☐ Transform the data and attach to mail as:

--- Select Export Format ---

[cancel](#)

[save](#)

2. Specify the following configuration details:

- **Name:** the name of the new task.
- **Description (optional):** the description of the new task.
- **From:** the account from which the email will be sent.
- **To:** the account to which the email will be sent.
- **Subject:** the subject of the email.
- **Body (optional):** the body of the email.
- **Data Export Format:** select the format of the email attachment:
 - No attachment.
 - Attach log data and configuration.
 - Attach log data in specific format (XML, CSV or TAB Delimited).

3. Click the 'save' link to save the new task definition.

Adding a new Export Module Task

1. Click the 'Export Module' link from the 'Tasks List' page.

Export Module

Export hierarchy

Select the modules and logs to export:

- ✓ ☐ Modules
- ▶ ☐ Examples

[cancel](#) [previous](#) [next](#)

2. Select modules and logs to be exported by the task.
3. Click the 'next' link.
4. Select the exporting media.

Export Module

Select exporting media

- [Zip and send by email](#)
- [Zip and send by ftp site](#)
- [Zip and copy to a local file system address](#)
- [Zip and copy to remote machine via SSH](#)

[cancel](#) [previous](#)

○ Zip and send by email

email log

Mail message

From	<input type="text" value="--- Select email account ---"/> new
To	<input type="text" value="--- Select email account ---"/> new
Subject	<input type="text"/>
Text	<div><div></div><div></div></div>

XpoLog will send the message with the zipped log attached to it.

[previous](#) [next](#)

- Specify the following configuration details:
 - **From:** the account from which the email will be sent.
 - **To:** the account to which the email will be sent.
 - **Subject:** the subject of the email.
 - **Text (optional):** the body of the email.
- Click 'next'.
- Specify the new task's name and description.
- Click 'save' to save the new task.

○ Zip and send by ftp site

export to FTP

FTP details

FTP Address	<input type="text" value="--- Select ftp account ---"/> new
Directory	<input type="text" value="/"/> (ftp site directory)

XpoLog will zip the log and copy it to the FTP location.

[previous](#) [next](#)

- Specify the following configuration details:
 - **FTP Address:** the account of the ftp site.
 - **Directory:** the directory the exported modules and logs will be uploaded to.
- Click 'next'.
- Specify the new task's name and description.
- Click 'save' to save the new task.

○ Zip and copy to a local file system address

Export to File System

File System Location

Directory [new](#) (File system address)
Overwrite ☒ (When unchecked XpoLog will create a new unique file name)
XpoLog will zip the log and copy it to the File system location.

[previous](#) [next](#)

- Specify the following configuration details:
 - **Directory:** the account pointing to the file system location to which the exported modules and logs will be saved.
 - **Overwrite:** indicates whether the zip file should overwrite a duplicate file or create a new file with unique name.
- Click 'next'.
- Specify the new task's name and description.
- Click 'save' to save the new task.

○ Zip and copy to remote machine via SSH

Export via SSH

SSH details

SSH Address [new](#)
Directory
XpoLog will zip the log and copy it to the specified location.

[previous](#) [next](#)

- Specify the following configuration details:
 - **SSH Address:** the SSH account of the remote host.
 - **Directory:** the directory the exported modules and logs will be uploaded to.
- Click 'next'.
- Specify the new task's name and description.
- Click 'save' to save the new task.

Adding a new JMS Message Task

1. Click the 'JMS Message' link from the 'Tasks List' page.

JMS Message Task

JMS Message details

Name	<input type="text"/>
Description	<input type="text"/>
JMS Account:	<input type="text" value="--- Select JMS account ---"/>
JMS message	<div><div></div></div>

General details

JMS Topic name	<input type="text"/>
JMS Queue Name	<input type="text"/>

[cancel](#)

[save](#)

- Specify the following configuration details:
 - Name:** the name of the new task.
 - Description (optional):** the description of the new task.
 - JMS Account:** the JMS account to be used.
 - JMS message:** the JMS message to be written.
 - JMS Topic name (optional if JMS Queue name was specified):** the name of the JMS topic the message should be written to.
 - JMS Queue name (optional if JMS Topic name was specified):** the name of the JMS queue the message should be written to.
- Click the 'save' link to save the new task definition.

Adding a new SNMP Trap Task

1. Click the ‘SNMP Trap’ link from the ‘Tasks List’ page.

SNMP Trap Task

SNMP Trap details

Name	<input type="text"/>
Description	<input type="text"/>
SNMP Account:	--- Select SNMP account --- ▾
SNMP Trap OID	<input type="text"/>
SNMP Community	<input type="text"/>

SNMP Trap variables

Add new variables

The following variable types are available:

Trap Time: the time of the SNMP trap. Specify the date format in the Message column, or leave empty for default date format (MM/dd/yyyy HH:mm:ss)

Log Time: the time of the event. Specify the date format in the Message column, or leave empty for default date format (MM/dd/yyyy HH:mm:ss)

Time: the value of a date column from the event. Specify the column name in square brackets. Add the date format after the column name (i.e: [Date;MM/dd/yyyy]) or leave empty for default date format (as configured in the log)

Text: free text or the value of any column from the event. Specify the column name in square brackets

Integer: the value of a number column from the event. Specify the column name in square brackets

Unsigned Integer: the value of a number column from the event. Specify the column name in square brackets

IP Address: the value of an IP address column from the event. Specify the column name in square brackets

Status: the status of the event

Existing Variables

OID	Name	Description	Type	Message
<div>cancel save</div>				

2. Specify the following configuration details:

- **Name:** the name of the new task.
- **Description (optional):** the description of the new task.
- **SNMP Account:** the account to be used.
- **SNMP Trap OID (optional for account of version 1):** the OID of the SNMP trap.
- **SNMP Community (optional):** the target community.

3. Specify the SNMP trap variables:

- Click the ‘Add new variables’ link.

Add new variables

☒ Select a predefined variable: --- Select variable --- ▾
☐ Create a custom variable:

OID	Name	Description	Type	Message	
<input type="text"/>	<input type="text"/>	<input type="text"/>	--- Select type --- ▾	<input type="text"/>	Add

The following variable types are available:

Trap Time: the time of the SNMP trap. Specify the date format in the Message column, or leave empty for default date format (MM/dd/yyyy HH:mm:ss)

Log Time: the time of the event. Specify the date format in the Message column, or leave empty for default date format (MM/dd/yyyy HH:mm:ss)

Time: the value of a date column from the event. Specify the column name in square brackets. Add the date format after the column name (i.e: [Date;MM/dd/yyyy]) or leave empty for default date format (as configured in the log)

Text: free text or the value of any column from the event. Specify the column name in square brackets

Integer: the value of a number column from the event. Specify the column name in square brackets

Unsigned Integer: the value of a number column from the event. Specify the column name in square brackets

IP Address: the value of an IP address column from the event. Specify the column name in square brackets

Status: the status of the event

- Add new variables, either by selecting from the predefined variables’ list or by specifying the custom details of the variable:
 - **OID:** the OID of the variable.
 - **Name:** the name of the variable.
 - **Description (optional):** the description of the variable.
 - **Type:** the type of the variable.

- **Message:** the message to be sent in the trap. This field is a dynamic field, which can contain placeholders which can be replaced with data from the log. The available placeholders are determined by the type of the variable in the following manner:
 - **Trap Time:** the time of the SNMP trap. Specify the date format in the Message column, or leave empty for default date format (MM/dd/yyyy HH:mm:ss).
 - **Log Time:** the time of the event. Specify the date format in the Message column, or leave empty for default date format (MM/dd/yyyy HH:mm:ss).
 - **Time:** the value of a date column from the event. Specify the column name in square brackets. Add the date format after the column name (i.e: [Date;MM/dd/yyyy]) or leave empty for default date format (as configured in the log).
 - **Text:** free text or the value of any column from the event. Specify the column name in square brackets.
 - **Integer:** the value of a number column from the event. Specify the column name in square brackets.
 - **Unsigned Integer:** the value of a number column from the event. Specify the column name in square brackets.
 - **IP Address:** the value of an IP address column from the event. Specify the column name in square brackets.
 - **Status:** the status of the event.
- Click the 'Add' link to add the new variable to the existing variables' list.
- 4. Click the 'save' link to save the new task definition.

Adding a new General Report Task

1. Click the 'General Report' link from the 'Tasks List' page.

General Reports Task

Task Details

Name

Description

Reports

all > server > Priorities Aggregation
all > server > Problems
Application > Columns
Application > Types
AppSrv01 > SERVERWINNode01 > server1 > http_access > Status + Remote Host (top 100)
AppSrv01 > SERVERWINNode01 > server1 > http_error > HTTP Severities

add
add all
remove
remove all

Reports to Run

☒ run report verifier tasks

[cancel](#)

[save](#)

2. Specify the following configuration details:
 - **Name:** the name of the new task.
 - **Description (optional):** the description of the new task.
 - **Reports:** select the report to be executed by the task.
 - **run report verifier tasks:** check to indicate that report verifiers should be executed as well.
3. Click the 'save' link to save the new task definition.

XpoSearch

Search Engine

Starting with version 2.7, XpoLog comes with a search engine that supports rapid textual search in logs. This enhanced search capability is integrated both in the log viewer (utilized by the filters and the quick search) and in a search engine screen that enables to search for text within multiple logs. The search engine search capability is based on an indexing mechanism that can run both automatically and upon user request. Only indexed logs are used by the search engine.

Running a Search

Click the Search Engine component to enter the search portal.

You can perform both simple, straightforward searches and advanced searches. For a simple search, simply enter the search term in the 'Search for' text box and press enter or click the 'go' link. Writing down a single word or a list of words will cause XpoLog to search all logs in which at least one of the words appear (OR operation). You can also define a regular expression as a search term. Searching a regular expression allows you to use wildcards anywhere within the search term, but it might cause for longer search times - especially if the wildcards appear at the beginning of the search term.

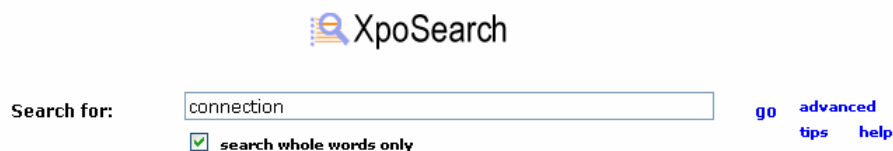


Figure ... - XpoSearch search portal

The result of a search query is a list of logs with indexing information and log information displayed next to each log result. By clicking on a search log result you drill down to that log's log view, where only records containing the search term are displayed. To get a merged view of the result logs select the 'Merge results' link in the results status line. Select the logs you want to participate in the merged result. By clicking the 'view' link, XpoLog will create a temporary merge log based on the selected logs and will show

it in the log view. Clicking the 'save and view' link will create and save the merge log and will then open its log view.

Search for: [go](#) [advanced](#)
☒ search whole words only [tips](#) [help](#)

Logs / [hide Merge results](#) Searched string: "connection" results 1 - 2 of 2 (0.469 seconds)

1. http_error (lastIndexed: 07/08/2007 12:10:24)
Module: server1
http_error_07.07.05_09.29.58.log (07/05/2007 09:29:58), http_error_07.07.14_05.27.09.log (07/14/2007 05:26:39), ...

2. SystemOut (lastIndexed: 07/08/2007 12:10:28)
Module: server1
SystemOut.log (07/17/2007 18:28:38)

Figure ... - Search result logs merged view

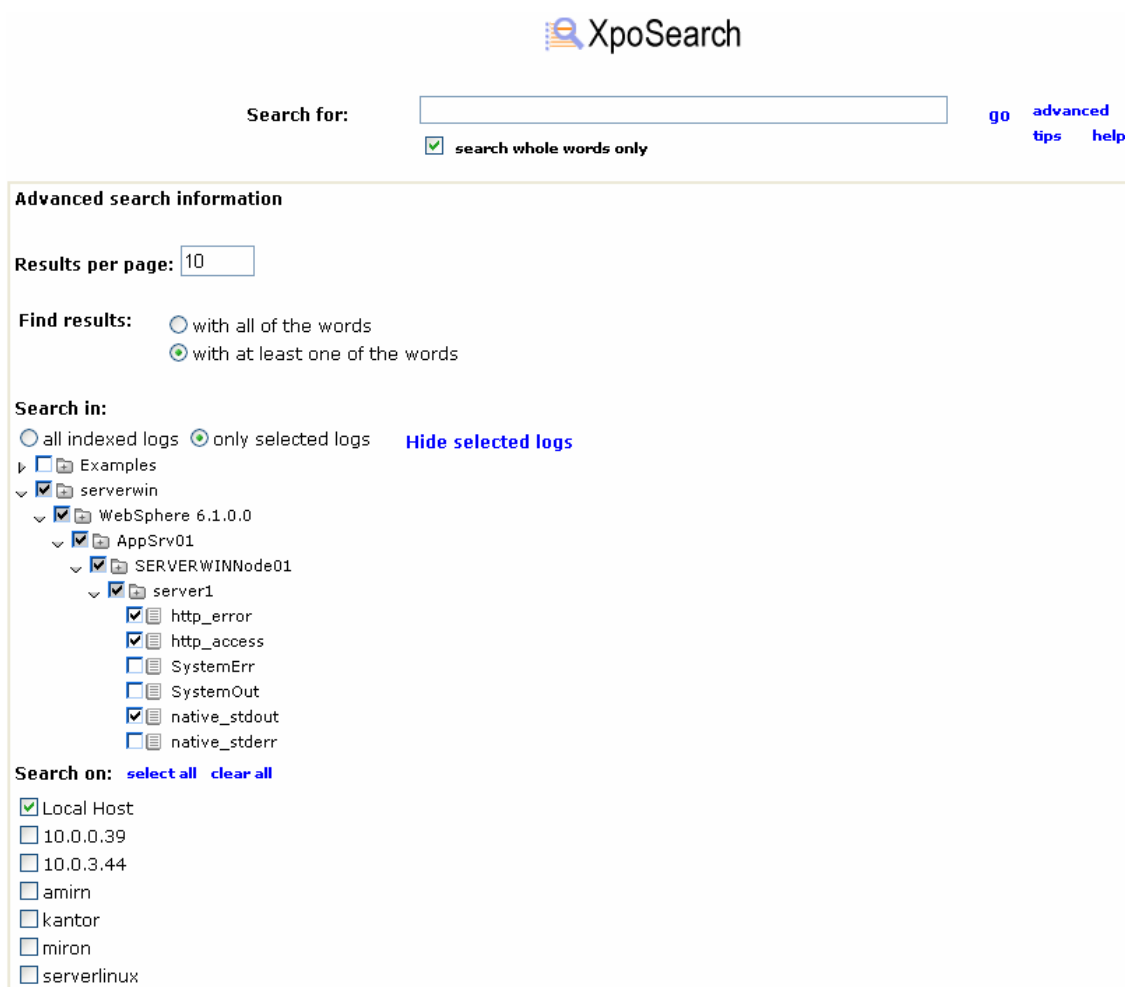
Clicking on the 'advanced' link will open the advanced search information section. If a different number results per page is desired, override the search engine default in the 'Results per page' entry.

If you want to search for logs where all the search terms appear, select in the 'Find Results' section the 'with all of the words' option. Otherwise use the 'with at least one of the words' option.

In the 'Search in' section, selecting 'only selected logs' will display the 'Select indexed logs' link that opens the logs tree. Only logs which use indexing and have been indexed will appear in that tree. Select the logs and modules to participate in the search. Click on the 'Hide selected logs' to hide the logs tree.

By default XpoLog searches the search term only within its own logs. To perform the

search also on logs residing in remote XpoLog nodes, select these nodes in the XpoLog nodes list in the 'Search on' section.



The image shows the 'XpoSearch' web interface. At the top, there is a search bar with the placeholder text 'Search for:' and a 'go' button. Below the search bar, there is a checkbox labeled 'search whole words only' which is checked. To the right of the search bar, there are links for 'advanced', 'tips', and 'help'. Below the search bar, there is a section titled 'Advanced search information'. This section contains a 'Results per page:' dropdown menu set to '10'. Under 'Find results:', there are two radio buttons: 'with all of the words' (unselected) and 'with at least one of the words' (selected). The 'Search in:' section has two radio buttons: 'all indexed logs' (unselected) and 'only selected logs' (selected). To the right of these radio buttons is a link 'Hide selected logs'. Below this, there is a tree view of the search scope. The tree starts with 'Examples' (expanded), then 'serverwin' (expanded), then 'WebSphere 6.1.0.0' (expanded), then 'AppSrv01' (expanded), then 'SERVERWINNode01' (expanded), then 'server1' (expanded). Under 'server1', there are several log types: 'http_error' (checked), 'http_access' (checked), 'SystemErr' (unchecked), 'SystemOut' (unchecked), 'native_stdout' (checked), and 'native_stderr' (unchecked). At the bottom, there is a 'Search on:' section with links 'select all' and 'clear all'. Below this, there is a list of nodes with checkboxes: 'Local Host' (checked), '10.0.0.39' (unchecked), '10.0.3.44' (unchecked), 'amirn' (unchecked), 'kantor' (unchecked), 'miron' (unchecked), and 'serverlinux' (unchecked).

Figure ... - Advanced search options

Running a search with a given search term will create a new 'user search result' entry that will be displayed in the 'Search Results' slide of the management pane on the left side of the screen. This way you can return to previously performed searches. Right click a search result and select 'Remove search' to remove it from the search results list, or click the small arrow in the 'Search Results' slide title and select 'Clear searches' to delete all pervious searches.

Administration

Click the 'XpoSearch' component to enter XpoLog's search engine. Select the 'Administration' menu to enter the 'Search Engine Management' screen. The search engine management information is organized in 4 tabs:

Log Selection

Select the logs you want to be indexed. Click 'save' to save your changes.

Global Scheduler

Set here the automatic execution of the global scheduler that will index logs for the first time. Select the 'Enable indexing scheduler' option to turn on the scheduler. See '[schedule information](#)' for more information on how to set a scheduler. The default indexing scheduling definition is to run every night, at 1 AM.

Delta Scheduler

Set here the automatic execution of the delta scheduler that will update the index of already indexed logs. Select the 'Enable delta indexing' option to turn on the scheduler. See '[schedule information](#)' for more information on how to set a scheduler.

General -

- Number of results per page: enter here the number of log results to be displayed in each result page of a search.
- Minimal file change: the minimal size in bytes of the changed or added portion of a log in order for the log to be indexed during delta scheduler executions.
- Average CPU Limitation: the average CPU consumption for indexing. Setting any value other than 'Unlimited' will influence the indexing performance.
- Indexing directory: either the default indexing directory or a user defined directory. Changing this setting will move all indexes to the selected directory; if this setting is done while a log is being indexed, that index will be deleted.
- Index numbers: check this value to enable indexing of numerical values.

Special characters: enter a sequence of all the characters that should serve as token delimiters and not be indexed. Use this option if you don't want to index certain characters. Since the indexed tokens are smaller in case special characters are used, the resulting indexing is smaller and the overall performance of the search engine increases.

Indexing

Log indexing is the process of scanning a log and creating an index - the structure that holds the information needed to quickly search for a text. In order to index a log, you need to turn on its 'use indexing' option. By default, all newly created logs have this option set. Most logs created by wizards also have this option set. Setting the 'use indexing' option can be done from 3 separate locations: from the [log administration](#), the [log customization](#) and the [search engine administration](#). Certain log types, such as remote logs, do not support indexing (remote logs could then be indexed on the XpoLog node on which they are defined).

Manual Indexing

On top of running log indexing using the scheduler as defined in the [search engine administration](#) you can also run logs indexing manually. To run manual indexing, do the following:

1. Click the 'XpoSearch' component and select the 'Indexing' menu to enter the 'Search Engine Indexing' screen.
2. Select from the logs tree the logs you want to index and click the 'run' link.
3. An 'indexing started running' message will be displayed. Press 'ok' to return to the indexing page. The status of the current log being indexed is displayed in the upper part of the view and in the log tree.

In the log view, if a filter was activated or a search term was entered and the log is set for indexing, a message prompting the user to run an index update will pop up in case the index is not up-to-date.

Search Engine Indexing

Indexed Logs

To **run indexing**, please check the logs you would like to run indexing on, and click run

- ✓ ☒ Examples
 - ☐ Client
 - ☐ Server
 - ☐ HTTP
 - ☒ sygatePacket
- ▶ ☐ serverlinux
- ▶ ☐ 10.0.0.9
- ▶ ☐ 10.0.0.20
- ▼ ☐ serverwin
 - ▼ ☐ WebSphere 6.1.0.0
 - ▼ ☐ AppSrv01
 - ▼ ☐ SERVERWINNode01
 - ▼ ☐ server1
 - ☐ trace
 - ☐ http_error - Indexed (08/07/2007 12:07:40)
 - ☐ http_access - Indexed (08/07/2007 12:07:44)
 - ☐ SystemErr - Indexed (08/07/2007 12:07:45)
 - ☐ SystemOut - Indexed (08/07/2007 12:07:45)
 - ☐ native_stdout - Indexed (08/07/2007 12:07:30)
 - ☐ native_stderr - Indexed (08/07/2007 12:07:45)
- ▶ ☐ AppSrv02
- ▶ ☐ IIS Web Server

Figure ... - Search engine indexing

Dashboard

Health view

XpoLog Dashboard is a component which allows you to get a high level picture of your entire system by displaying an overview of the health state of the different components in your system. Health is measured both in the occurrence of log events correlating to certain problems in your system ('risk') and in anomalies in log files - such as in the case where many events are suddenly written to a log file, something that may denote a problem in that log file's application. The dashboard's user interface enables the user to drill down both in the components resolutions (traversing an application by its modules tree, finally getting to the applications logs and their filters) and the time frame displayed (drill down from a time frame of one month to a day and then to an hour). From the component's lowest level (a log, a log's filter or a log's column) you can drill down directly to the log view of that log and continue your analysis there.

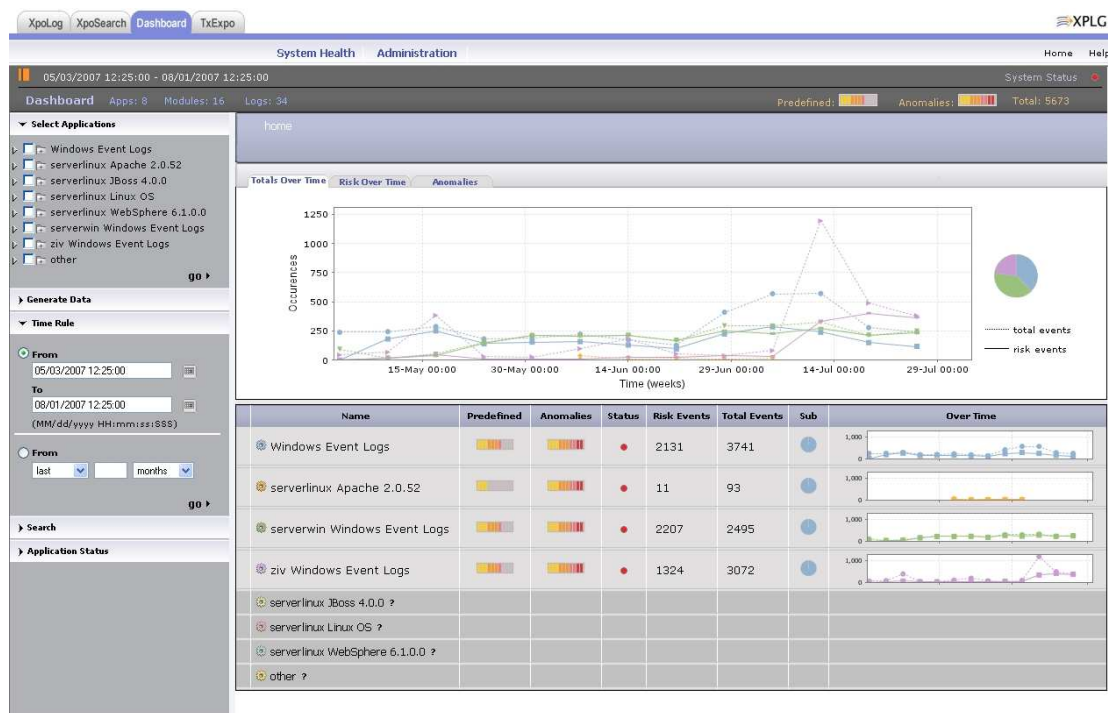


Figure ... - System Health Screen

The first time you enter the health view screen (by selecting 'Dashboard' from the portal or by clicking the 'Dashboard' tab) XpoLog collects the dashboard data based on the time frame defined in the dashboard administration; collecting the health view data might take

a couple of minutes, based on the amount of data. If you leave the health view screen the current display setup is saved, so next time you enter it you get the same view.

The health view screen is divided into three panes:

- The upper pane displays general information about your system, such as the number of applications, modules and logs defined, a general status indication, indications for the level of risk and anomalies, and the time frame of the viewed dashboard.
- The left pane is a control pane that comprises of five slides – for selecting the viewed applications, for setting the time rules for displayed and generated data, for entering a search query and for displaying the top level (application level) health state of your system. Use this control pane to navigate both in time and both between applications.

Select Applications

This slide displays the application tree of your system: applications, modules, and logs in a hierarchical view.

- Selecting a root for the displayed data: simply click on any component in the tree. The view in the main pane will be refreshed accordingly.
- Correlating the health state between different components: select the desired components from the tree and click ‘go’. The view in the main page will refresh showing only the selected components, as the figure below illustrates:



Figure ... - Correlated System Health View of Windows Event Logs

Generate Data

Use this slide to define the time frame to generate new data for. Enter either 'from/to' values or enter 'last/previous' data to define the time frame. If you want to generate data on selected components only, select them in the tree above and check the 'only selected apps' option; otherwise leave this option unselected. To start generating data, click the 'go' link.

Generating data might take a while, depending on the amount of data in your logs, the time frame set and the components selected.

The figure bellows demonstrated the settings for generating data for the last 3 months for the applications 'serverlinux Apache 2.0.52', 'serverlinux JBoss 4.0.0' and 'serverlinux Linux OS':

The screenshot shows a 'Generate Data' dialog box. It has two main sections: 'Select Applications' and 'Generate Data'. In the 'Select Applications' section, there is a tree view with the following items: 'Windows Event Logs', 'serverlinux Apache 2.0.52', 'serverlinux JBoss 4.0.0', 'serverlinux Linux OS', 'serverlinux WebSphere 6.1.0.0', 'serverwin Windows Event Logs', 'ziv Windows Event Logs', and 'other'. The first four items are checked. A 'go' button is at the bottom right of this section. The 'Generate Data' section has two radio buttons: 'From' and 'To'. The 'From' radio button is selected, and it has a date field showing '07/05/2007 00:00:00'. The 'To' radio button is also selected, and it has a date field showing '07/12/2007 00:00:00'. Below these fields is a format string '(MM/dd/yyyy HH:mm:ss)'. There is also a 'From' radio button with a dropdown menu showing 'last', a text field with '3', and a dropdown menu showing 'months'. At the bottom, there is a checkbox labeled 'only selected apps' which is checked, and a 'generate' button.

Figure ... - Generate Data

Time Rule

The 'Time Rule' slide is used to define a new time frame for the viewed data. Set the time frame exactly as you set the time frame for data generation and click 'go' to refresh the view. Notice that missing data will not be generated – only already available data for the specified time frame will be processed and displayed.

Search

Enter here a search phrase and click 'go' to get the search results in a new XpoLog page.

Application Status

This slide displays a summary of the system health of the upper most level the components tree – the applications. Clicking an application has the same affect as clicking an application in the application tree – setting the application to be the root of the system health display in the main pane.

Main Page

The main pane consists of two parts: the upper one shows an over (main) time graph of the selected mode (totals over time, risk over time and anomalies), and the lower part contains a table with information and graphs of the children of the selected component. If you click on a node in the main graph you will drill down to the time frame displayed in that node's tool tip as show below:

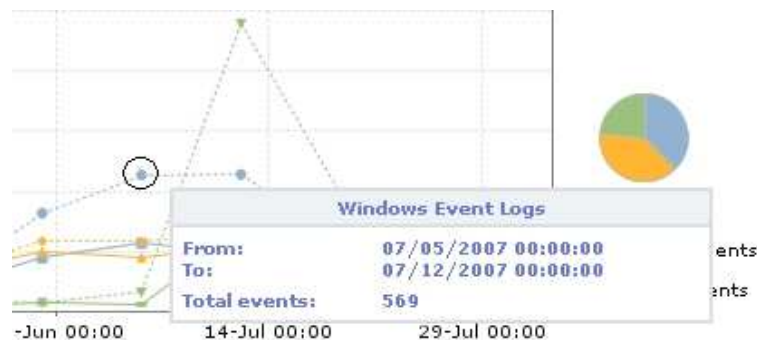


Figure ... - Graph Node Tool Tip Data

Clicking on the marked node will result in the following view:



Figure ... - Time Frame Zoom In

Do return to the pervious time frame, simple click on the arrow next the 'Totals Over Time' tab.

The entries in the table below the graph are divided into two groups: the components with a light grey background are those with data (although the might have no risk or anomalies). The components with a dark grey background are those for which no system health data is available. To generate data for these components, select them in the components tree in the control pane on the left, enter the time frame desired in the 'Generate Data' slide (**not** the 'Time Rule' slide) and press 'go'. When hovering with the mouse of the question mark next to a component for which no data is available, an appropriate message is displayed as shown in the picture below:

serverwin Windows Event Logs	[Bar Chart]	[Bar Chart]	[Red Dot]	228
ziv Windows Event Logs	[Bar Chart]	[Bar Chart]	[Red Dot]	33
serverlinux JBoss 4.0.0 ?	<div>No data available for Application serverlinux_JBoss_4.0.0 Use left pane to generate new data</div>			
serverlinux Linux OS ?				
serverlinux WebSphere 6.1.0.0 ?				
other ?				

Figure ... - No Data Message

Administration

As described earlier, the system health is measured both in terms of risk and in terms of anomalies. Both risk and anomaly definitions can be set for each and every log in your system.

Defining log risks

Risks for a log are defined as the occurrence of certain events in that log. For instance, the occurrence of an access log event with a 404 status may denote that an illegal request has been submitted. Or an event of an error log with a priority "FATAL" means something pretty bad happened in your application.

To isolate these events, XpoLog uses a set of filters, each corresponding to an event or a multitude of events. From the log view select from the log navigation bar the filter's menu by pressing the small arrow next to the filter's "go" link. Select "edit" to edit an already defined filter or "new" to create a new one. For more information on defining filters, see [Filter Definition](#). In the filter definition page, the last section is called "System Health". This is where you set the risk level that corresponds to the occurrence of (one or more) events defined by that filter. The lowest risk is 1 and the highest is 10. If the event denoted by that filter does not mean any risk to your system, leave the risk weight at "None". For instance, in an error log containing priorities, you might set a filter called "FATAL" by selecting the "FATAL" entry of the "Priorities" section in the filter definition page, and set the risk weight to be 10.

To complete the System Health definition enter the condition for the given risk weight by selecting the number of events and the operation (more then, less then, equals and not equals). The condition defines the number of occurrences of that log within the minimal time frame of **5 minutes**. For instance if the occurrence of at least 5 error events in an error log in a time frame of five minutes means a risk weight of 8, select 8 at the risk weight, "More Then" in the next combo box and enter "4" in the text box to complete your definition.

Log's configurations in XpoLog generated either by the detection wizard or by running an application wizard have already their risk levels set for their predefined filters. You can always edit these filters to change their risk level or enter new filters with new risk

levels that correspond to events you consider risky.

The picture below displays an example of setting such a filter:

Priorities

From name: DEBUG, INFO, WARN, ERROR, FATAL

To name: FATAL

add, add all, remove, remove all

Date and Time

☒ Dates limit

☐ Show records that arrive **after** 08/01/2007 13:41:51 [calendar](#) (MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH:mm:ss:SSS)

☐ Show records that arrive **before** 08/01/2007 13:41:51 [calendar](#) (MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH:mm:ss:SSS)

☐ show records from the last [] hours []

Text

Show records that	contain	the text	match whole words	case sensitive	regular expression
Show records that	contain	the text	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show records that	contain	the text	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show records that	contain	the text	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show records that	contain	the text	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☒ search in all columns

☐ search in these columns

Columns: Date, Thread, Priority, Logger, Code, Message

Only: []

add, add all, remove, remove all

System Health

Risk Weight: 10 if there are More Than 0 records in a time frame of 5 minutes.

[save](#) [cancel](#) [help](#)

Figure ... - Defining Log Risks

In the [dashboard administration screen](#) you can set the risk weights of multiple filters together. To set risk levels for multiple filters, do the following:

1. Select the 'Dashboard' component and then 'Administration' from the top menu to enter the dashboard's administration page.
2. In the 'System Filter Rules' set the system health as described above, select from the logs' tree the filters you want this health setting to apply to and click 'save'. If you want to set further risk setting for other filters, just repeat these steps and click 'save' again.

System members

System Filter Rules Thresholds Time Rule

System Health

Risk Weight: if there are records in a time frame of 5 minutes.

Filter Rules Selection

- ☒ Modules
 - ☐ Examples
 - ☐ station
 - ☐ remote
 - ☒ Windows Event Logs
 - ☒ serverwin
 - ☒ WebLogic 10.0
 - ☒ wl_server
 - ☒ examplesServer
 - ☒ examplesServer
 - ☒ Filters
 - ☐ Error creating Runtime MBean for JVM (risk - 7.0)
 - ☒ Failed to listen on port port0, failure count: fails1, failing for secs2 seconds, e3 (risk - 7.0)
 - ☐ Referenced global pool (global) has the same name as a locally defined connection pool or data source (local) (risk - 5.0)
 - ☐ Server subsystem serverService failed (risk - 9.0)
 - ☐ Unable to delete configuration MBean for pool 'poolName': 'err' (risk - 4.0)
 - ☐ A JDBC pool connection leak was detected (risk - 6.0)
 - ☐ A JMS message consumer could not be created using a temporary queue or topic that was created using another connection
 - ☐ A JMS session pool could not be created because the propName property was not specified
 - ☐ A PooledConnectionFactory object with an invalid external version of version was found
 - ☒ A globally scoped connection pool named (poolName) already exists (risk - 5.0)
 - ☐ A malformed WebLogic Object Name has been reported.
 - ☒ A mismatch exists between the bean code and generated code.ejbName . Please rerun ejbc on the bean code.
 - ☐ A mismatch exists between the number of components specified, specifiedComponents, and the number of components that exist
 - ☐ A partial update of an archived application is not allowed. Application app cannot be redeployed.

3.

Figure ... - Setting risk weight for multiple logs

Defining log statistics

Anomalies are defined as deviations in terms of the number of occurrences with relation to previously computed averages. Statistics for logs is computed for every hour of the week and takes into account both the number of total events of the log and the number of unique occurrences of values for selected log columns ("Column statistics"). For more information on statistics and anomalies, see the 'Defining log statistics' section of the help.

In order to set the statistics parameters of a certain log, do the following:

1. Go to the log's edit wizard. See 'Log Configuration' for more details on how to define logs. Click 'next' in the Log's general definition's page to get to the 'Log pattern administration' page and click 'next' again here to get to the 'Log field admin' page.
2. In the 'statistics settings' section, select the 'Compute statistics' option to enable statistical evaluation of the log. When this option is selected, the 'Compute statistics' combo box is displayed next to each of the log's fields (columns). For

each column you want statistics (and anomalies) to be computed for select one of the following options:

- 'Do not compute' – no statistics (and no anomaly) will be computed for this column.
- 'Compute unique values' – statistics will be computed for each of this column's values.
- 'Compute average' – only the average of the occurrences of unique values will be computed. Anomaly for each unique value is then computed based on this average statistics.

Selecting 'compute unique values' for a column where many unique values are expected will result in large statistics data and less accurate anomalies, so always consider in these cases using 'compute average'. In the image below statistical evaluation for the log was turned on, average statistics computation was defined for the 'Source IP' column and unique values statistics computation was defined for the 'Status' column

Log field admin

Generated table

Source IP	Remote Logical Username	Remote User	Date	Method	URL	Protocol	Status	Request Time (Millis)
10.0.3.10	-	-	10/Jun/2007:13:53:52 +0300	GET	/index.html?id=25	HTTP/1.1	200	259031 "-" ** IE 6.0 **
10.0.3.10	-	-	10/Jun/2007:13:53:52 +0300	GET	/1.htm	HTTP/1.1	200	259031 "serverlinux/index.html?id=25" **
10.0.3.10	-	-	10/Jun/2007:13:53:55 +0300	GET	/2.htm	HTTP/1.1	200	259032 "serverlinux/1.htm" ** IE 6.0 **

Field specification

Field Type	Field Name	Index this column	Compute statistics	Compute statistics
1. string	Source IP	<input checked="" type="checkbox"/>	Index this column	compute average
2. string	Remote Logical Username	<input checked="" type="checkbox"/>	Index this column	do not compute
3. string	Remote User	<input checked="" type="checkbox"/>	Index this column	do not compute
4. date	Date	<input checked="" type="checkbox"/>	Index this column	do not compute
5. string	Method	<input checked="" type="checkbox"/>	Index this column	do not compute
6. string	URL	<input checked="" type="checkbox"/>	Index this column	do not compute
7. string	Protocol	<input checked="" type="checkbox"/>	Index this column	do not compute
8. number	Status	<input checked="" type="checkbox"/>	Index this column	compute unique values
9. string	Request Time (Millis)	<input checked="" type="checkbox"/>	Index this column	do not compute

Virtual columns [Add virtual column](#)

Statistics settings

☒ Compute statistics
set this option to enable statistical evaluations on this log

Indexing settings

☒ Use indexing
using log indexing enables rapid search and filtering; indexed logged can be used in Xpolog Search Engine

☐ Use indexing for date search
set this option to allow for quick date search using the index

[cancel](#) [previous](#) [next](#)

Figure 1 – Defining Log Statistics

Creating Dashboard Data:

There are 3 means for creating dashboard data:

- The first mean for creating dashboard data is by running the automatic configuration wizard. Once applications have been selected by the user and their configurations (their corresponding modules, logs and reports) created (steps 1 and 2 of the wizard), the wizard can continue to generate the dashboard data. Just press the 'Next' link to run both the reports of the created applications and the dashboard data generator. XpoLog will generate report data for each of the applications' reports for the last day, while the dashboard data generator will run on the applications' log data of the last month. To set a different time frame for the generation of the dashboard data, click, before pressing the 'Next' link, the 'Advanced' link and enter a different time rule - either in terms of from/to dates or in terms of previous/last days.
- The second mean for creating dashboard data is from the system health's control pane, as described above.
- The third mean for creating dashboard data is by setting the dashboard scheduler. To set the dashboard scheduler, do the following:
 1. After the dashboard component has been selected, select the 'Administration' menu.
 2. Click the 'Time Rule' tab to display the dashboard generation and display time rules.
 3. In the 'Health report execution' section set the time frame you want the dashboard data to be generated for. In the 'Run health and statistics on the pervious' entry set the time unit and the time amount (for instance 1 day - pervious day, or simply yesterday) to define that time frame.
- In the 'Scheduling' section, set the data do define when the dashboard data generation should occur. Select either the days of the weeks in which the execution should take place, or enter instead the days of the month and the desired months in which you want your job to run.

After defining the days at which your job should be executed you define the time of the desired executions. You can enter either a specific time (in the 'Activate on the given hour' section) or define hours interval and minutes interval, so that on the selected days the operation will be executed in the given hours intervals and within each hour in the given minutes interval. For example, selecting in the

scheduling section 'Every month' and 'Every day' and then defining to iterate every three hours and within each hour every 20 minutes will cause the job to be executed every day at 00:20, 00:40, 01:00, 03:00, 03:20 and so on.

System members

System Filter Rules Thresholds Time Rule

Health report execution

Run health and statistics on the previous days

☒ Enable dashboard execution scheduler.

☒ Scheduling

☐ Activate at specific days every week

☐ Sun. ☐ Mon. ☐ Tues. ☐ Wed. ☐ Thurs. ☐ Fri. ☐ Sat.

☒ Activate at specific days in months

On month at day (s)

Activate on the given hour

On every scheduled day activate the task at

: : (hour:minutes:second)

Hours and minutes intervals

iterate every hours for each activation day

iterate every minutes for each activation hour

Default time filter for health state display

☐ Dates limit

☐ Show records that arrive **after** (MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH:mm:ss:SSS)

☐ Show records that arrive **before** (MM/dd/yyyy HH:mm:ss, MM/dd/yyyy HH:mm:ss:SSS)

☒ show records from the last days

[cancel](#)

[save](#)

Figure ... - Setting Dashboard Scheduler